

10/758,023  
TOMUCHIKA MURAKAMI ET AL  
IMAGE PROCESSING METHOD AND IMAGE  
PROCESSING APPARATUS

CFM 03401  
US



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

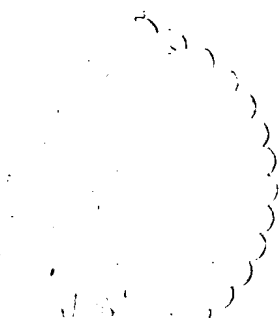
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    4 月    9 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 1 0 5 4 9 8  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 1 0 5 4 9 8 ]

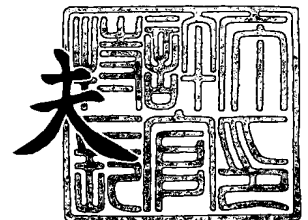
出      願      人                      キヤノン株式会社  
Applicant(s):



2 0 0 4 年    1 月 1 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 1 1 1 2 6 9

【書類名】 特許願

【整理番号】 254018

【提出日】 平成15年 4月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明の名称】 画像処理方法

【請求項の数】 1

【発明者】

    【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会  
社内

    【氏名】 村上 友近

【発明者】

    【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会  
社内

    【氏名】 若尾 聡

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100076428

    【弁理士】

    【氏名又は名称】 大塚 康德

    【電話番号】 03-5276-3241

【選任した代理人】

    【識別番号】 100112508

    【弁理士】

    【氏名又は名称】 高柳 司郎

    【電話番号】 03-5276-3241

## 【選任した代理人】

【識別番号】 100115071

【弁理士】

【氏名又は名称】 大塚 康弘

【電話番号】 03-5276-3241

## 【選任した代理人】

【識別番号】 100116894

【弁理士】

【氏名又は名称】 木村 秀二

【電話番号】 03-5276-3241

## 【先の出願に基づく優先権主張】

【出願番号】 特願2003- 12514

【出願日】 平成15年 1月21日

## 【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102485

【プルーフの要否】 要

【書類名】 明細書  
【発明の名称】 画像処理方法  
【特許請求の範囲】

【請求項 1】 第 1 の領域と第 2 の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第 1 の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第 2 の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、画像に対して改竄された位置や改竄の有無を検出するための技術に関するものである。

【 0 0 0 2 】

【従来の技術】

近年、従来の銀塩写真や 8mm フィルムに変わって、撮影した情報をデジタル化し、デジタルデータとして記録媒体等に記録するデジタルカメラといった映像入力装置が実用化されている。これにより、撮影した情報そのものをパーソナルコンピュータを始めとする情報処理装置に移し、表示させることが可能になった。また、このような映像データを通信回線を利用することで全国どこでも瞬時に映像データを送信することも可能になった。

【 0 0 0 3 】

そのため、事故処理で証拠写真を扱う保険会社や建築現場の進捗状況の記録を

扱う建設会社においてデジタル映像データの利用が考えられている。しかし一方で目覚ましいデータ処理技術の進歩により、映像データを始めとしたデジタルデータの編集をフォトタッチツールや動画編集ツール等の使用で容易に行うことが可能になった。そのため、デジタル映像データの信頼性は従来の銀塩写真等と比較して低く、証拠としての能力に乏しいという問題があった。

#### 【 0 0 0 4 】

その為、デジタルデータに対する原本性を実現する為の技術や改ざん位置を検出する為の技術が数多く開発されてきた。

#### 【 0 0 0 5 】

改ざん検出の技術は一般に大きく分けて二つのアプローチが考えられる。一つはデジタルデータのデータ部分からハッシュ関数を用いて算出したダイジェスト（ハッシュ値）を秘密鍵で暗号化（署名生成）して生成されるデジタル署名をファイルの所定位置（ヘッダ等）に添付するデジタル署名技術である。

#### 【 0 0 0 6 】

もう一方は、一定の規則性を満たす電子透かしをデジタルデータ自体に埋め込み、一定の規則性が満たされているかを検証することでデジタルデータの改ざんの有無や改ざん位置の検出を行う電子透かし技術である。

#### 【 0 0 0 7 】

前者のデジタル署名技術では、画像検証の為のデジタル署名はファイルの所定位置（ヘッダ等）に添付される為、ファイルフォーマット変換によりヘッダの情報が失れた場合、フォーマット変換されたファイルからは改ざん検出ができないというデメリットがある。

#### 【 0 0 0 8 】

一方、後者の電子透かし技術では、一定の規則性を満たす電子透かしをデジタルデータ自体に埋め込む為、ファイルフォーマット変換には耐性があるものの、画質劣化をもたらすという課題がある。

#### 【 0 0 0 9 】

次に、従来の改ざん位置検出用電子透かしについて述べる。従来では、改ざん位置検出用電子透かし埋め込み装置においては、入力画像データを画素毎にふた

つの領域（例えば、8ビットグレースケール画像なら上位7ビットと最下位ビット）に分割し、埋め込み処理対象画素毎に所定の鍵情報から画素位置に依存して生成される乱数と対応する画素位置の一方の画像領域のデータ（例えば上位7ビット）を暗号化関数に入力し、画素毎に透かし情報（1ビット）を生成する。そして生成された透かし情報（1ビット）を対応する分割した他方の画像領域（例えば最下位ビット）のデータと置き換える。この操作を入力画像の全画素に対して行い、改竄位置検出用の電子透かしの埋め込みを行う。

#### 【0 0 1 0】

改ざん位置検出装置においては、埋め込み時と同じく、入力画像データを画素毎にふたつの領域に分割し、検証処理対象画素毎に、所定の鍵情報から画素位置に依存して生成される乱数と対応する画素位置の一方の画像領域のデータ（例えば上位7ビット）を暗号化関数に入力し、画素毎に透かし情報（1ビット）を生成する。そして生成された画素毎の透かし情報（1ビット）と対応する分割した他方の画像領域のデータ（例えば最下位ビット）と比較し、ビット値が異なれば改竄、同じであれば改竄が行われていないと見なす。この操作を入力画像の全画素に対して行い、画像中の改ざん位置を検出する。

#### 【0 0 1 1】

透かしデータは、画素毎に、画素位置に応じて鍵情報から生成される乱数と一方の画像領域のデータから、暗号化関数を用いて1または0のバイナリーデータとして生成される為、1か0かが反転する場合にのみ改ざんを検出することが出来る。本方式は、アルゴリズムが公開されても良いというメリットがあるものの、所定の鍵情報から生成される乱数が流出すれば、改ざんされていないと見なされる改ざん画像が容易に生成可能な為、この乱数を秘密情報とする必要がある。

#### 【0 0 1 2】

また他の従来例では、改ざん位置検出用電子透かし埋め込み装置においては、画像データをふたつの領域に分割し、一方の画像領域から擬似階調画像を生成する。次に擬似階調画像に対し秘密の鍵情報を用いてランダム位置に並べ替えるランダム化処理を行い、埋め込み位置が画像全体に拡散した透かし画像データを生成する。最後に透かし画像を他方の画像領域と置き換え、改ざん位置検出用の透



かしが埋め込まれた画像を出力する。

#### 【 0 0 1 3 】

改ざん位置検出装置では、まず、透かし入りの改ざん画像をふたつの領域に分割し、一方の領域の画像データを取得する。次に、一方の領域の画像データに対し秘密の鍵情報を用いて、埋め込み位置を逆にランダム化し、擬似階調画像を復元する。そして透かし入りの改ざん画像から他方の領域の画像データを取得し、再び擬似階調画像を生成する。

#### 【 0 0 1 4 】

最後に、改ざん画像の一方の領域から復元された擬似階調画像と、他方の領域の画像データから生成された擬似階調画像を比較し、改ざん位置を特定する。

#### 【 0 0 1 5 】

本方式は、アルゴリズムが公開されても良いというメリットがあると共に、復元された擬似階調画像から、元の画像状態が分かるという更なるメリットがある。しかしながら、改ざん時に破損箇所が逆ランダム化により画像全体に散乱する為、正確な改ざん位置が特定できないというデメリットがある。

#### 【 0 0 1 6 】

##### 【発明が解決しようとする課題】

上記後者の従来例による手法では、元の画像状態が分かるというメリットがあるものの、正しい改ざん位置が特定できないという課題があった。

#### 【 0 0 1 7 】

また上記に述べた従来の電子透かし技術を用いた場合、改ざん位置を特定することができるものの、改ざん位置検出用の電子透かしを埋め込む際に必要な鍵情報と改ざん位置検出の際に必要な鍵情報は同一である為、改ざん位置検出の為の鍵情報は、第三者に流出すると容易に改ざんが可能となる為、オープンにすることが出来ず、限定された人物や機器でしか、画像の検証を行うことが出来ない不便さがあった。

#### 【 0 0 1 8 】

本発明は以上の問題に鑑みてなされたものであり、画像に対する改竄の位置を正確に検出することを目的とする。

**【0019】****【課題を解決するための手段】**

本発明の目的を達成するために、例えば本発明の画像処理方法は以下の構成を備える。

**【0020】**

すなわち、第1の領域と第2の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第1の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第2の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする。

**【0021】****【発明の実施の形態】**

以下添付図面を参照して、本発明を好適な実施形態に従って詳細に説明する。なお、本発明の手法と従来技術との違いを明確に示す為、はじめに従来技術の説明を行う。

**【0022】**

図15は従来技術であるコンピュータセキュリティシンポジウム2002で発表された論文「改ざん前の状態が分かるデジタル画像の改ざん検出用電子透かし法」の改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。なお、以降の説明では、論文「改ざん前の状態が分かるデジタル画像の改ざん検出用電子透かし法」を論文(1)と呼ぶこととする。

**【0023】**

まず、各画素の画素値が8ビットで表現されるグレースケール画像は、領域取



得部 1501 に入力され、LSB を除く上位 7 ビットのビットプレーンを画像領域 A として、後段の特徴抽出部 1502 に出力する。次に特徴抽出部 1502 では、画像領域 A に対して、シミュレーティッドアニーリングを用いた方法を用い、2 値画像（2 次元特徴画像）を後段のランダムイズ部 1505 に出力する。

#### 【0024】

ここで、代表的な擬似階調画像の作成法の一つに誤差拡散法があるが、誤差拡散法は擬似階調値と原画像の画素値の誤差を順に伝播させながら擬似階調値を計算していく為、改ざん箇所の擬似階調の計算が他の部分の擬似階調の計算に影響を及ぼす。従って改ざん場所の特定が出来なく成る為、特徴抽出部における処理として適さない。前述の論文で用いているシミュレーティッドアニーリング法は原画像と 2 値画像の視覚的差異をエネルギー関数としてシミュレーティッドアニーリングアルゴリズムによりエネルギーが最小（正確には極小）となる 2 値画像を求める方法であり、改ざん箇所の擬似階調の計算は、他の部分の擬似階調の計算に影響を与えないというメリットがある。

#### 【0025】

次に、ランダムイズ部 1505 では、入力された 2 値画像（2 次元特徴画像）に対し、並びをランダム化する処理を行い、並びがランダム化された 2 値画像（2 次元特徴画像）を後段の置換部 1506 に入力する。

#### 【0026】

最後に置換部 1506 では、入力画像の LSB のビットプレーンを、ランダムイズ部から入力されるランダム化された 2 値画像に置き換え、透かし入り画像を生成する。

#### 【0027】

図 16 は論文（1）における改ざん位置検出装置の機能構成を示すブロック図である。

#### 【0028】

まず、改ざんが施された改ざん画像は分離部 1601 に入力される。分離部 1601 では、入力画像を画像領域 A（LSB を除く上位 7 ビットのビットプレーン）と画像領域 B（LSB のビットプレーン）に分離し、それぞれ後段の特徴抽

出部 1605 と逆ランダマイズ部 1602 に出力する。

#### 【0029】

次に逆ランダマイズ部 1602 では、分離部 1601 から入力された画像領域 B、すなわち 2 値画像（LSB のビットプレーン）に対し、改ざん位置検出用電子透かし埋め込み装置におけるランダマイズ部 1505 と逆のランダム化処理を行い、原画像の特徴を表す一部が破壊された 2 値画像を後段の比較部 1606 に出力する。このとき論文（1）では、改竄が検出不能な改ざん画像を生成させない為に逆ランダマイズ部 1602 における並び換えのための情報を秘密の鍵情報として保つ必要がある。

#### 【0030】

次に特徴抽出部 1605 では、入力された画像領域 A（LSB を除く上位 7 ビットのビットプレーン）に対し、改ざん位置検出用電子透かし埋め込み装置における特徴抽出部 1502 と同様の処理を行い、改ざん画像の特徴が抽出された 2 値画像を生成し、後段の比較部 1606 に出力する。

#### 【0031】

比較部 1606 では、逆ランダマイズ部 1602 から入力される原画像の特徴を表す一部が破壊された 2 値画像と特徴抽出部 1605 から入力される改ざん画像の特徴が抽出された 2 値画像とを比較し、改ざん位置を特定する。しかし、論文（1）では既に簡単に述べたが、以下に述べるような改ざん位置を誤る課題がある。

#### 【0032】

論文（1）では、改ざん位置検出装置において、逆ランダマイズ部 1602 に入力される改ざん画像の画像領域 B は、改ざん操作によって一部が破壊される可能性が高い。一部が破壊された画像領域 B は、ランダム化処理により、破壊された部分を画像全体に拡散するため、誤りが画像全体に散乱された 2 値画像を得ることが出来る。しかし、比較部 1606 で画像領域 A から算出される 2 値画像（2 次元特徴画像）と比較する時、誤りが画像全体に散乱している為、正確な改ざん位置を特定することが出来ず、実際には改ざんされていない画像位置に対して改ざんを検出する可能性がある。

**【 0 0 3 3 】**

次に、本発明に係る画像処理装置を改竄位置検出用電子透かし埋め込み装置、改竄位置検出装置に適用した実施形態について説明する。

**【 0 0 3 4 】****[第 1 の実施形態]****<改ざん位置検出用電子透かし埋め込み装置>**

はじめに、公開鍵、即ち誰でも入手可能な鍵で改竄位置検出が可能な電子透かしの埋め込みを行う電子透かし埋め込み装置について説明する。

**【 0 0 3 5 】**

図 1 は改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

**【 0 0 3 6 】**

図 2 は、1 画素が 8 ビットから成る入力画像をビットプレーン毎に示した図である。説明を分かりやすくするため、本実施形態では、入力画像は図 2 に示すような 1 画素 8 ビットからなるグレースケール画像であるとする。

**【 0 0 3 7 】**

以下、図 1 を参照して、改竄位置検出用電子透かし埋め込み装置が行う処理について説明する。

**【 0 0 3 8 】**

まず、入力画像（以下、原画像と呼称する場合もあり、例えば縦 5 1 2 画素×横 5 1 2 画素とする）は、領域取得部 1 0 1 に入力される。領域取得部 1 0 1 では、入力画像から所定の画像領域 A を取得し、後段の特徴抽出部 1 0 2 に入力する。説明を分かりやすくするため、領域取得部 1 0 1 では、入力画像の最下位（LSB）のビットプレーン（図 2 に示したビットプレーン 2 0 2）を除く上位 7 ビットのビットプレーン（図 2 に示したビットプレーン群 2 0 1）を画像領域 A として取得するとする。

**【 0 0 3 9 】**

次に、特徴抽出部 102 では、入力された画像領域 A の画像、即ち入力画像の上位 7 ビットのビットプレーンで表現される画像を用いて入力画像の特徴を表現した 2 次元特徴画像を出力する。

#### 【0040】

図 3 は入力画像、2 次元特徴画像、そして後述するランダム化された誤り訂正符号化暗号化透かし情報によって表現される画像を示す図である。

#### 【0041】

特徴抽出部 102 から出力される 2 次元特徴画像は、同図に 302 で示すように、入力画像 301 よりも縦横の大きさが小さな 1 ビットの画像となる。詳しくは後述するが、これは、2 次元特徴画像を暗号化、誤り訂正符号化した後でも画像領域 B（本実施形態では入力画像の LSB）に収まるようにするためである。

#### 【0042】

特徴抽出部 102 で行われる処理の一例としては、画像領域 A に値が全てゼロの LSB を追加することで、各画素の画素値が 8 ビットで表現される画像を生成し、更にこの画像の縦横のサイズを半分に縮小し、縮小した画像の各画素値を所定のマトリクス（例えばベイヤーマトリクスなど）の値と比較することで 2 値化する（組織的ディザ処理）といった処理が考えられる。またディザ処理ながら高品位な 2 値画像が得られるブルーノイズマスク法なども存在する。その他には輪郭抽出処理もあげられる。また論文（1）で述べられるシミュレーティッドアニーリング法を特徴抽出部 102 で用いてもよい。

#### 【0043】

入力画像が文書画像の場合にはレイアウト解析及び OCR 処理を施し、文字情報や 2 次元レイアウトを格納可能な文章フォーマットに、OCR で抽出した文字やレイアウト情報を格納し、2 次元特徴画像としてもよい。以上のように、特徴抽出部 102 において行われる処理は様々な種類が設計可能である。

#### 【0044】

特徴抽出部 102 において行われる好ましい処理は、入力画像全体の特徴を抽出できることと、一部を局所的に変化させた入力画像から作成される 2 次元特徴画像は、局所的に変化させた箇所以外は元と変わらない 2 次元特徴画像を作成で

きることである。

#### 【0045】

図3の301は入力画像のイメージ図であり、302は2次元特徴画像のイメージ図である。本実施形態では2次元特徴画像を生成するために、入力画像に対する縦横のサイズを半分に縮小し、2値化処理するが、縮小処理や2値化処理は必ずしも必須の処理ではなく、画像領域Bに2次元特徴画像を納める十分なサイズがあれば、等倍の大きさの2次元特徴画像を生成してもよいし、多値階調の2次元特徴画像を生成してもよい。

#### 【0046】

次に、2次元特徴画像を暗号化部103に入力する。暗号化部103ではまず、入力される2次元特徴画像と種々のデータを必要に応じて組み合わせ、改ざん位置検出用透かし情報を生成する。以降、「透かし情報」あるいはwは改ざん位置検出用透かし情報を表すとする。

#### 【0047】

図8は「透かし情報」の概略構成を示す図である。同図には801～804の複数の「透かし情報」の構成例を示しているが、「透かし情報」の内部構成は801～804の構成例に限定されないものとする。

#### 【0048】

2次元特徴画像と組み合わせる種々のデータとしては、図8の801に示すような正しい復号化が行われたかチェックする目的の「検査ビット」や802に示すような2次元特徴画像の縦と横の長さを2進数で表す「縦長」、「横長」、2次元特徴画像を生成する際に用いた特徴抽出処理を特定する情報の1つである「特徴抽出処理ID」などがあげられる。さらに図示しないが、「2次元特徴画像のビット長」や「撮影日時」やGPSから得られる「位置情報」や「撮影デバイスのシリアル番号」、「撮影者情報」などを追加してもよい。

#### 【0049】

検査ビットは少なくとも2次元特徴画像を含む透かし情報の一部（2次元特徴画像や「縦長」、「横長」、「特徴抽出処理ID」等の情報）の整合性を検証する為のビット情報であり、例としては、少なくとも2次元特徴画像を含む透かし

情報の一部をハッシュ関数に入力して得られるハッシュ値が挙げられる。ハッシュ関数は、入力値が僅かな変化に対しても、大きく異なる固定長の値を返す性質がある。従って、ハッシュ値を用いた検査ビットを用いれば、僅かな変化に対しても高い精度で整合性の検証が行うことが可能である。また検査ビットとして2次元特徴画像に誤りが無いかを調べるチェックサム（検査合計）を用いることも可能である。

#### 【0050】

次に暗号化部103では、生成された透かし情報に対して、暗号化処理を施す。暗号化部103では、様々な暗号方式が利用可能であるが、公開鍵暗号方式を用いる場合、秘密鍵を所有する人物や機器でなくとも、対応する公開鍵で改ざん位置検出が可能になるという大きなメリットを実現できる。その為、本実施形態では公開鍵暗号方式に従って暗号化処理を行うものとする。しかし、暗号化部103で共通鍵暗号方式を用いることも可能である。このとき、改ざん位置の検出は共通鍵を持った人物や機器でしか行えないデメリットがあるが、共通鍵暗号方式を用いる場合、公開鍵暗号方式に比べ高速に処理できるメリットもある。

#### 【0051】

既に周知の技術であるので詳しい説明は省くが、公開鍵暗号方式では、秘密鍵を用いて暗号化されたデータは公開鍵で容易に復号可能であるが、秘密鍵を知らない限り公開鍵で復号できる正しく整合性の取れたデータを生成することは実質不可能である。

#### 【0052】

従って、秘密鍵がデジタルカメラやデジタルビデオカメラなどの撮像デバイス内部で読み出されないように厳重に管理されているなら、秘密鍵に対応する公開鍵で復号可能な改ざん後の画像データと対応する2次元特徴画像を含む暗号化した透かし情報を生成することは実質不可能である。なお、公開鍵暗号方式としては、RSA暗号や楕円暗号などがよく知られている。

#### 【0053】

暗号化部103では透かし情報に対し公開鍵暗号方式を用いて秘密鍵で暗号化（署名生成）を行い、暗号化透かし情報を出力する。以降、C（w）は暗号化透

かし情報を表すとする。

#### 【 0 0 5 4 】

ここで暗号化透かし情報  $C(w)$  の情報量について考える。暗号化部 1 0 3 から出力される暗号化透かし情報  $C(w)$  は、入力データである透かし情報  $w$  と比べてデータの大きさが変化する可能性がある。例えば、暗号化部で RSA 暗号を用いた場合、透かし情報  $w$  は鍵長の単位で処理される為、 $C(w)$  は鍵長に比例した長さとなる。

#### 【 0 0 5 5 】

今、暗号化部 1 0 3 で用いる RSA 暗号の鍵長を 1 0 2 4 ビットとし、暗号化部 1 0 3 に入力される 2 次元特徴画像は各画素 1 ビットの縦 2 5 6 画素、横 2 5 6 画素（6 5 5 3 6 ビット）であり、検査ビットが 2 次元特徴画像から計算される 1 6 0 ビットのハッシュ値であるとする、暗号化部 1 0 3 に入力される透かし情報は 6 5 6 9 6 ビットとなる。既に述べたように、RSA 暗号では、鍵長の単位で入力データを処理する為、最後の 1 0 2 4 ビットに満たないビット情報（1 6 0 ビット）に対しては所定のビット値（例えばゼロ）が付加（パディング）されて 1 0 2 4 ビット単位で処理される。従って、暗号化部 1 0 3 から出力される暗号化透かし情報  $C(w)$  のビット長は鍵長の整数倍となり、6 6 5 6 0 ビットとなる。

#### 【 0 0 5 6 】

このように、暗号化処理時に透かし情報の末尾に所定のビット（例えばゼロ）が付加される場合、復号時の透かし情報でも透かし情報の末尾に所定のビット（例えばゼロ）が付加されている。予め 2 次元特徴画像のサイズが分からないときには、透かし情報に含められる情報である「縦長」「横長」（透かし情報の構成が図 8 中の 8 0 2 や 8 0 4 に示す構成である場合）を利用し、2 次元特徴画像データの長さを計算することで、透かし情報中に含まれている 2 次元特徴画像を正しく抽出できる。

#### 【 0 0 5 7 】

また、透かし情報は暗号化処理を行う前に鍵長の整数倍にパディング処理されてから暗号化処理を施されるが、その際にパディングするビットを予め決められ

た固定のビットとすることで、パディングするビットに「検査ビット」と同様の役割を兼ねさせることも可能である。

#### 【0 0 5 8】

次に、暗号化透かし情報  $C(w)$  は、誤り訂正符号化部 1 0 4 に入力される。誤り訂正符号化部 1 0 4 では入力された暗号化透かし情報  $C(w)$  に対し、誤り訂正符号化処理を行い、誤り訂正符号化暗号化透かし情報を出力する。以降、 $CC(C(w))$  は誤り訂正符号化暗号化透かし情報を表すとする。

#### 【0 0 5 9】

誤り訂正符号化部 1 0 4 で用いる誤り訂正符号としては、BCH符号、リードソロモン符号、畳み込み符号、ターボ符号など様々な符号が存在するが、予想される改ざん、即ち発生する誤りの種類により、適切な誤り訂正符号を用いるとよい。

#### 【0 0 6 0】

一般に誤りの種類として、ビット毎に独立に発生する「ランダム誤り」や部分的に集中して連続的に発生する誤り「バースト誤り」や、所定のビットからなる小ブロック（バイトと呼ぶ）毎に発生する「バイト誤り」などがある。「ランダム誤り」には「BCH符号」、「バイト誤り」には「リードソロモン符号」が有効であるといわれている。なお、「リードソロモン符号」で符号化した後にインターリーブ処理（例えばランダム化処理）を加えることで、「バースト誤り」に強くすることが可能である。なお、インターリーブ処理としてはランダム化処理に限らず、情報系列の並びを攪拌する為の種々の方式や設計が存在する。本実施形態ではインターリーブ処理としてランダム化処理を例に説明を行うが、インターリーブ処理は情報系列の並びを攪拌する処理とし、ランダム化処理に限らないとする。

#### 【0 0 6 1】

画像の改ざんとしては、一般に画像の特定の箇所に集中した改ざんが想定される。従って画像に対して「バースト誤り」に強い符号を用いた誤り訂正符号化を行うことで、特定の箇所に集中した改ざんを「バースト誤り」として検出することができる。



**【0062】**

しかし「バースト誤り」に強い符号を用いずとも、暗号化透かし情報C (w) を符号化後にインターリーバでランダム化処理を施すことで、「バースト誤り」に強くすることも可能である。なお、このとき誤り訂正符号を復号側では、誤り訂正符号化暗号化透かし情報ECC (C (w)) に対して誤り訂正復号処理を行う前にデインターリーバで逆ランダム化処理を施し、符号化ビット列の順序を元に戻してから復号する必要がある。

**【0063】**

図6はそれぞれ透かし情報(601)、暗号化透かし情報(602)、誤り訂正符号化透かし情報(603)、ランダム化誤り訂正符号化透かし情報(604)のビット長を比較、説明するための概略図である。

**【0064】**

誤り訂正符号化暗号化透かし情報603は、冗長なビットが誤り訂正の目的で加算される為、暗号化透かし情報602と比べ、情報量(同図ではビット長に反映されている)が増加している。

**【0065】**

誤り訂正符号化部103における誤り訂正符号化のパラメータは、暗号化透かし情報ECC (C (w)) の情報量が画像領域B(第1の実施形態ではLSBのビットプレーン)に正確に収まる情報量になるように設計するとよい。例えば、誤り訂正符号のパラメータを固定にして、暗号化された透かし情報量にパディング処理を施して、誤り訂正後に画像領域Bに正確に収まる情報量にしてもよいし、パディング処理ではなくチェックサムなどを加え、より正確に誤り訂正復号を行えるようにしてもよい。また、誤り訂正符号のパラメータをパディングやチェックサムなしに、誤り訂正符号化後に画像領域Bに正確に収まる情報量になるように誤り訂正符号部103におけるパラメータを設定しても良い。

**【0066】**

図7は誤り訂正符号化を行う前の透かし情報C (w) の一例を示す図である。図7では、誤り訂正符号化後に画像領域Bに正確に収まるように、末尾に所定のビット(例えば0)をパディングしてあるが、このとき、誤り訂正符号化を行う

前の暗号化透かし情報C (w) に、暗号化透かし情報のビット長を記すビット列を「暗号化透かし情報のビット長」の位置に2進数で記録すれば、仮にパディングが存在したとしても、暗号化された透かし情報の部分のビット列を正しく抽出することも出来る。

#### 【0067】

誤り訂正符号化104では、暗号化透かし情報C (w) のサイズが小さいほど(即ち、2次元特徴画像の情報が少ないほど)誤り訂正符号化部104で冗長性を生かし誤り訂正の能力を強力にすることが出来る。

#### 【0068】

その結果、透かしが埋め込まれた画像に対して大きな改ざんが施された場合でも、改ざん位置の特定が可能となる。逆に2次元特徴画像の情報が多いほど、誤り訂正符号化部104で強い誤り訂正を行うことが出来なくなる。

#### 【0069】

2次元特徴画像の情報量と誤り訂正符号の強さ(改ざんに対する強さ)はトレードオフの関係にあるので、本実施形態によれば、用途に応じて2次元特徴画像の情報量と誤り訂正符号の強度パラメータを決定することが出来る。このように用途に応じてパラメータを柔軟に設定できる点は、本実施形態の大きな長所の一つである。2次元特徴画像の情報量と誤り訂正符号の強度パラメータは、経験的に得られるデフォルトパラメータで設定してもよいし、撮像デバイスで撮影画像に応じて自動的に決定してもよいし、また改ざん位置検出用電子透かしの埋め込み時にユーザに選択させても良い。

#### 【0070】

次に、誤り訂正符号化暗号化透かし情報ECC (C (w)) は、インターリーバ105に入力される。インターリーバ105では、入力された誤り訂正符号化暗号化透かし情報ECC (C (w)) を構成するビット列をランダムに並べ替える操作を行い、ランダム化された誤り訂正符号化暗号化透かし情報を出力する。このとき並べ替えに用いる鍵情報は改ざん位置検出時にも必要となるが、本実施形態においてはこの鍵情報を用いても改ざんが不可能であるため、公開情報としてよい。

## 【0071】

なお、インターリーバ105は必ずしも必須のブロックではなく、誤り訂正符号化部104で特定の箇所に集中した改ざん（バースト誤り）に対しても誤り訂正能力がある誤り訂正符号を用いる場合やターボ符号のように誤り訂正符号内部にインターリーバの機能を有している誤り訂正符号を用いる場合には不要である。

## 【0072】

以降、 $S(ECC(C(w)))$ はランダム化された誤り訂正符号化暗号化透かし情報を表すとする。

## 【0073】

最後に、インターリーバ105でランダム化された誤り訂正符号化暗号化透かし情報 $S(ECC(C(w)))$ は、置換部106に入力され、入力画像の所定の画像領域B（本実施形態では図2の202に相当するLSBのビットプレーン）と置き換えが行われ、ランダム化された誤り訂正符号化暗号化透かし情報 $S(ECC(C(w)))$ が埋め込まれた透かし入り画像を出力画像として出力する。

## 【0074】

図3の303は、置換部106でLSBのビットプレーンと置き換えられるランダム化された誤り訂正符号化暗号化透かし情報 $S(ECC(C(w)))$ をラスタ順に並べ、画像として表現した場合のイメージ図である。暗号化処理や誤り訂正符号化処理により、情報量が2次元特徴画像302に比べて増大している。

## 【0075】

例えば、入力画像を縦512画素×横512画素の各画素8ビットのグレースケール画像とし、2次元特徴画像は縦256画素×横256画素の各画素1ビットのモノクロ画像とし、誤り訂正符号化暗号化透かし情報 $S(ECC(C(w)))$ は縦512画素×横512画素の各画素1ビットのモノクロ画像とすると理解しやすい。

## 【0076】

### ＜改ざん位置検出装置＞

次に改ざん位置検出装置について詳しく説明する。図4は改ざん位置検出装置の機能構成を示すブロック図である。同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

#### 【0077】

図5は、改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。以下、図4のブロック図に従って、図5を用いながら、改ざん位置検出装置が行う処理を説明する。

#### 【0078】

図5において501は改竄がなされた画像を示し、510の領域（網掛けされた三日月の形状の領域）が改竄がなされた領域を示す。以下の説明では501に示す改竄画像を例に取り説明するが、各種の改竄画像に対しても以下説明する処理は適用可能である。

#### 【0079】

改ざん画像501（入力画像）は、改ざん位置の検証の為、分離部401に入力される。分離部401では入力画像を画像領域Aと改ざん位置検出用の透かし情報が埋め込まれている画像領域Bに分離する。本実施形態では、埋め込み装置と同じく、図2に示すように画像領域Aは最下位（LSB）のビットプレーンを除く上位7ビットのビットプレーン201とし、画像領域BはLSBのビットプレーン202とする。

#### 【0080】

図5において502は、入力画像から得られる画像領域Bを示す画像データである。入力画像から得られる画像領域Bの画像データは502に示すように、改ざん位置（520で示す領域の位置）で破壊されている可能性がある。

#### 【0081】

次に、分離部401で分離された画像領域Bのデータは、デインターリーバ402に入力される。デインターリーバ402では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報S'（ECC（C（w）））を構成する各ビ

ット列の並びを、元のビットの並びに戻す処理を行う。

#### 【0082】

デインターリーバ402はランダム化を解除した一部が壊れた誤り訂正符号化暗号化透かし情報（以降、 $ECC'(C(w))$ と表現する）を後段の誤り訂正復号化部403に出力する。なお、誤り訂正符号の種類によっては、埋め込み時にインターリーバを必要としない場合がある。従って、デインターリーバ402における処理は必須ではなく、埋め込み時にインターリーバ105で $ECC(C(w))$ をランダム化した場合にのみ必要となる。

#### 【0083】

次に、デインターリーバ402から出力される $ECC'(C(w))$ は、誤り訂正復号部403に入力される。誤り訂正復号部403では入力された一部が破壊された $ECC'(C(w))$ に対して誤り訂正復号を行い、暗号化された透かし情報 $C(w)$ を後段の暗号復号部404に出力する。

#### 【0084】

ここで、画像領域Bの透かしデータが改ざんにより大きく破壊され、誤り訂正符号が正しく誤り訂正復号が出来ない場合（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある）、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を終了する。

#### 【0085】

次に暗号復号部404に入力された誤り訂正復号された暗号化透かし情報 $C(w)$ は、公開鍵暗号方式で、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵を用いて、暗号化透かし情報 $C(w)$ を復号化し、透かし情報 $w$ を復元する。

#### 【0086】

改ざん位置検出に用いる公開鍵が正しいとき、暗号復号部404では、透かし情報 $w$ を構成する検査ビットの値をチェック（検査ビットが2次元特徴画像のハッシュ値である場合は、透かし情報 $w$ に含まれる2次元特徴画像からハッシュ値を計算し、透かし情報 $w$ 中の検査ビットと一致するか否かを比較）することで、

正しい秘密鍵で暗号化（署名生成）された暗号化透かし情報C（w）であるか、異なる秘密鍵で暗号化（署名生成）された暗号化透かし情報C（w）であるかを識別することが出来る。公開鍵暗号方式では、秘密鍵の知識がなければ、公開鍵で復号できる正しく整合性の取れた透かし情報を生成することは出来ない。

#### 【0087】

従って、検査ビットの値が一致しないならば、暗号化透かし情報C（w）は正しい秘密鍵で暗号化されていないことを意味する。そこでこのような場合は、「不正な改ざんが行われている」旨をユーザに通知し、処理を終了する。なお、改ざん位置検出に用いる公開鍵を誤って用いた場合にも検査ビットの値は誤るので、「復号に用いる鍵が異なる」旨をユーザに通知してもよい。

#### 【0088】

暗号復号部404では図6の601に相当する、暗号化が解除された透かし情報wの中から2次元特徴画像を取り出し、後段の比較部406に出力する。図5の504は、改ざん画像の画像領域B502から復元された2次元特徴画像を示す。図5の504に示すように、透かし情報wの中から取り出された2次元特徴画像は、上記原画像に対する相似画像である。

#### 【0089】

なお、暗号復号部404で復号された透かし情報に「特徴抽出処理ID」が含まれている場合には、特徴抽出処理IDに基づき、特徴抽出部405で行う特徴抽出処理の種別を決定するなどしてもよい。

#### 【0090】

次に特徴抽出部405では、分離部401から入力される画像領域Aに対し、特徴抽出処理を行う。このとき、特徴抽出処理は透かし埋め込み時に生成した2次元特徴画像の生成方法と同じ処理である。そして、特徴抽出部405は特徴抽出処理によって得られる2次元特徴画像を後段の比較部406に出力する。

#### 【0091】

図5の503は改ざん画像から上記特徴抽出処理によって得られる2次元特徴画像を示す。このとき図5の503に示すように、改ざん画像から計算された2次元特徴画像は、改ざんを反映した2次元特徴画像となることが想定される（同

図に示した例では、入力画像 5 0 1 における改竄領域 5 1 0 が反映されている改竄領域 5 3 0 として反映されている）。

#### 【 0 0 9 2 】

最後に比較部 4 0 6 では、暗号復号部 4 0 4 から入力される正しく復元された 2 次元特徴画像と特徴抽出部 4 0 5 から入力される改ざん情報が反映された 2 次元特徴情報を比較し、2 つの 2 次元特徴画像の間で値が異なる箇所（即ち、改竄の位置）を画像の検証者に示す。図 5 の 5 0 5 は 2 次元特徴画像 5 0 3 と 2 次元特徴画像 5 0 4 の差分を表す画像（2 次元特徴画像 5 0 3 と 2 次元特徴画像 5 0 4 とで対応する画素の画素値の差分の集合による画像）である。比較部 4 0 6 は例えば、差分画像 5 0 5 を生成し、表示部にこの差分画像 5 0 5 を表示させることで、改ざん位置を画像の検証者に視覚的に示すことが出来る。

#### 【 0 0 9 3 】

また、改ざん画像から計算された 2 次元特徴画像 5 0 3 と画像領域 B から復元された 2 次元特徴画像 5 0 4 を一覽表示させることで、差分画像 5 0 5 のように改ざん位置を視覚的に検証者に対して提示するだけではなく、2 次元特徴画像上でどの位置が原画像と比べて変化したかという改ざんの内容を画像の検証者に視覚的に明確に示すことが可能になる。

#### 【 0 0 9 4 】

図 5 の 5 0 6 は、差分画像 5 0 5 を改ざん画像 5 0 1 の大きさに拡大し、改ざん画像 5 0 1 上に重ね合わせて（オーバーレイして）表示した画像である。このようにすることで、視覚的に改ざん位置を分かり易く表示することも可能である。このとき、2 次元特徴画像の縦横の大きさが入力画像よりも小さい場合、画像 5 0 6 のように、改ざん位置は厳密に 1 画素単位で特定出来ないが、大きな改ざんの場合、実用上十分効果がある。

#### 【 0 0 9 5 】

従来技術である論文（1）で述べられた手法と第 1 の実施形態に係る手法とを対比して考えると、従来技術においてランダムイズ部 1 5 0 5 は本実施形態におけるインターリーバ 1 0 5 に相当する機能を実行していることが分かる。また、本実施形態の改ざん位置検出用電子透かし埋め込み装置に存在する暗号化部 1 0

3 および誤り訂正符号化部 1 0 4 に相当する機能は、従来技術の論文（1）では存在しないことが分かる。

#### 【0 0 9 6】

また、改ざん位置検出装置でも同様に、従来技術において逆ランダムイズ部 1 6 0 2 は本実施形態におけるデインターリーバ 4 0 2 に相当する機能を実行していることが分かる。また、本実施形態の改ざん位置検出用電子透かし埋め込み装置に存在する誤り訂正復号化部 4 0 3、暗号復号部 4 0 4 に相当する機能は、従来技術の論文（1）では存在しないことが分かる。

#### 【0 0 9 7】

本実施形態では誤り訂正符号を導入することで従来技術の論文（1）と比べて、改ざん位置をより正確に特定し、更に公開鍵暗号化を導入することで安全性と利便性の高い改ざん位置検出システムを実現していることが分かる。

#### 【0 0 9 8】

以上、本実施形態では、“アルゴリズム公開”かつ“秘密情報を用いずに画像の改ざん位置判定が可能”である改ざん位置検出用透かし埋め込み方法および改ざん位置検出方法について詳しく述べた。

#### 【0 0 9 9】

なお、本実施形態は、改ざん前と改ざん後の画像から同じ 2 次元特徴画像が生成されるような僅かの改ざんの場合、改ざんの有無を検出することが出来ない。しかし、僅かな変更を改ざんから見なさないロバスト性を実現した僅かな変化に対してロバストな画像検証方法であると言える。これは従来技術の論文（1）においても実現できなかった技術である。

#### 【0 1 0 0】

画像に影響のない僅かな変化に対して改ざんの有無の検出する必要がある場合は、追加の手段、例えば、画像データ全体をハッシュ関数に入力し、ダイジェスト（ハッシュ値）を計算し、そのダイジェスト（ハッシュ値）を秘密鍵で暗号化（署名生成）し、画像ファイルのヘッダなどの所定位置にデジタル署名として添付する方法でも実現可能である。

#### 【0 1 0 1】



## [第 2 の実施形態]

## &lt;改ざん位置検出用電子透かし埋め込み装置&gt;

本実施形態に係る埋め込み装置は、第 1 の実施形態に係る埋め込み装置によって生成される透かし情報に、画像領域 A を用いて計算されるダイジェスト（ハッシュ値）を更に加える処理を行う。これにより、画像の改ざん位置だけでなく、画像の改ざんの有無も判定可能にする。

## 【0 1 0 2】

図 9 は本実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。なお同図において、図 1 に示したものと同一のものについては同じ番号を付けており、その説明を省略する。また、同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

## 【0 1 0 3】

図 9 において図 1 と大きく異なる点は新たにハッシュ算出部 9 0 7 が追加された点である。また、暗号化部 9 0 3 は、暗号化部 1 0 3 が行う処理と同様の処理を行って第 1 の実施形態で説明した透かし情報を生成し、この透かし情報に更にハッシュ算出部 9 0 7 が生成したハッシュ値のデータを含める処理を行う。

## 【0 1 0 4】

以下、図 9 を用いて本実施形態における改ざん位置検出用電子透かし埋め込み装置を説明する。なお第 1 の実施形態と同様の処理を行うブロックについては説明を簡素化する。

## 【0 1 0 5】

まず、第 1 の実施形態と同じく入力画像は、領域取得部 1 0 1 に入力される。領域取得部では、入力画像から所定の画像領域 A を取得し、後段の特徴抽出部 1 0 2 および後段のハッシュ算出部 9 0 7 に入力する。本実施形態でも説明を分かりやすくするため、画像領域 A は最下位（LSB）のビットプレーンを除く上位 7 ビットのビットプレーンとする。

## 【0 1 0 6】

次に特徴抽出部 1 0 2 では、入力された画像領域 A、即ち上位 7 ビットのビッ

トプレーンを用いて入力画像の特徴を抽出し、2次元特徴画像を出力する。

#### 【0107】

次に、ハッシュ算出部907では、画像領域Aの画像データをハッシュ関数に入力し、ダイジェストを生成し、後段の暗号化部903に入力する。

#### 【0108】

ここでハッシュ関数について簡単に説明を行う。ハッシュ関数とは可変長データを入力とし、固定長のデータ（ダイジェスト又はハッシュ値と呼ぶ）を計算して出力する関数であるが、主に以下のような特徴を持つ。

#### 【0109】

- (1) 入力データ長が異なっても、固定長のダイジェストを出力
- (2) 入力データが僅かに異なれば、出力ダイジェストは大きく異なる
- (3) ダイジェストから元の入力データを生成できない
- (4) 同じダイジェストを出力する入力データを検出することは困難

現在、代表的なハッシュ関数としては、MD2、MD4、MD5、SHA-1などがある。SHA-1の場合、出力ダイジェストのサイズは160ビット（20バイト）である。上記のようなハッシュ関数においては、画像領域Aの一部を改ざんした場合に、同じダイジェストを得られる確率は非常に低く、ダイジェストを用いれば画像の僅かな改ざんでも容易に検出できる。

#### 【0110】

次に、暗号化部903では、特徴抽出部102から入力される2次元特徴画像及びハッシュ算出部907から入力されるダイジェスト、検査ビットなどを組み合わせ、図8の803に示すような、改ざん位置検出用透かし情報を生成する。なお、必要に応じて、第1の実施形態で述べたような「横長」「縦長」「特徴抽出処理ID」などを記録するビット領域を設けてもよい。

#### 【0111】

次に暗号化部903では、生成された透かし情報に対して暗号化処理を施す。暗号化部903では第1の実施形態と同じく公開鍵暗号方式を用い、透かし情報に秘密鍵で暗号化（署名生成）を行い、暗号化透かし情報C（w）を出力する。

#### 【0112】

次に、暗号化透かし情報  $C(w)$  は、誤り訂正符号化部 1 0 4 に入力される。誤り訂正符号化部 1 0 4 では入力された暗号化透かし情報  $C(w)$  に対し、誤り訂正符号化処理を行い、誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  を出力する。

#### 【0 1 1 3】

次に誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  は、インターリーバ 1 0 5 に入力される。インターリーバ 1 0 5 では入力された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  に対し、ビット列をランダムに並べ替える操作を行い、ランダム化された誤り訂正符号化暗号化透かし情報  $S(ECC(C(w)))$  を後段の置換部 1 0 6 に出力する。なお、第 1 の実施形態と同じく、インターリーバ 1 0 5 は必ずしも必須のブロックではなく、誤り訂正符号化部 1 0 4 で特定の箇所に集中した改ざんに対しても誤り訂正能力がある誤り訂正符号を用いる場合やターボ符号のように誤り訂正符号内部にインターリーバの機能を有している誤り訂正符号を用いている場合には不要である。

#### 【0 1 1 4】

最後に、インターリーバ 1 0 5 でランダム化された誤り訂正符号化暗号化透かし情報  $S(ECC(C(w)))$  は、置換部 1 0 6 に入力され、入力画像の所定の画像領域  $B$  (本実施形態では図 2 の 2 0 2 に相当する  $LSB$  のビットプレーン) と置き換えが行われ、ランダム化された誤り訂正符号化暗号化透かし情報  $S(ECC(C(w)))$  が埋め込まれた透かし入り画像を出力画像として出力する。

#### 【0 1 1 5】

##### <改ざん位置検出装置>

次に本実施形態に係る改ざん位置検出装置について説明する。図 1 0 は本実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。なお同図において、図 4 に示したものと同一のものについては同じ番号を付けており、その説明を省略する。また、同図に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

## 【0116】

図10において図4と大きく異なる点は新たにハッシュ算出部1007が追加された点である。また、比較部1006は第1の実施形態に係る比較部406が行う処理に加えて、ダイジェストを用いた改竄の有無を通知する処理も行う。以下、図10を用いて本実施形態に係る改ざん位置検出装置について説明する。なお第1の実施形態と同様の処理を行うブロックについては説明を簡素化する。

## 【0117】

まず、図5の501に示されるような改ざんが施された画像は、分離部401に入力される。分離部401では入力画像を画像領域Aと改ざん位置検出用の透かし情報が埋め込まれている画像領域Bに分離する。本実施形態では、埋め込み装置と同じく、図2に示すように画像領域Aは最下位(LSB)のビットプレーンを除く上位7ビットのビットプレーン201とし、画像領域BはLSBのビットプレーン202とする。このとき画像領域Bから得られる画像は画像の改ざんにより、図5の502に示すように、改ざん位置で破壊されている可能性がある。

## 【0118】

次に、分離部401で分離された画像領域Bのデータは、デインターリーバ402に入力される。デインターリーバ402では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報 $S'$  ( $ECC(C(w))$ )を元のビットの並びに戻す処理を行う。デインターリーバ402はランダム化を解除した一部が壊れた誤り訂正符号化暗号化透かし情報、即ち $ECC'(C(w))$ を後段の誤り訂正復号化部403に出力する。

## 【0119】

なお、誤り訂正符号の種類によっては、埋め込み時にインターリーバを必要としない場合がある。従って、デインターリーバ402における処理は必須ではなく、埋め込み時にインターリーバ105で $ECC(C(w))$ をランダム化した場合にのみ必要となる。

## 【0120】

次に、デインターリーバ402から出力される $ECC'(C(w))$ は、誤り

訂正復号部 4 0 3 に入力される。誤り訂正復号部 4 0 3 では入力された一部が破壊された ECC' (C (w)) に対し、誤り訂正復号処理を行い、暗号化された透かし情報 C (w) を後段の暗号復号部 4 0 4 に出力する。

#### 【0 1 2 1】

ここで、画像領域 B の透かしデータが改ざんにより大きく破壊され、誤り訂正符号が正しく誤り訂正復号が出来ない場合、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を中止する。（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある。）

次に暗号復号部 4 0 4 に入力された誤り訂正復号された暗号化透かし情報 C (w) は、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵暗号方式で公開鍵を用いて暗号化透かし情報 C (w) を復号化し、透かし情報 w を復元する。

#### 【0 1 2 2】

透かし情報 w に検査ビットがある場合は、透かし情報 w を構成する検査ビットの値をチェック（検査ビットが 2 次元特徴画像のハッシュ値である場合は、透かし情報 w に含まれる 2 次元特徴画像からハッシュ値を計算し、透かし情報 w 中の検査ビットと一致するか否かを比較）することで、正しい秘密鍵で暗号化（署名生成）された暗号化透かし情報 C (w) であるか、異なる秘密鍵で暗号化（署名生成）された暗号化透かし情報 C (w) であるかを識別することが出来る。検査ビットの値が一致しないならば、暗号化透かし情報 C (w) は暗号化（署名生成）が行われた秘密鍵で暗号化されていないことを意味し、「不正な改ざんが行われている」旨を結果表示し、処理を終了する。

#### 【0 1 2 3】

暗号復号部 4 0 4 は暗号化が解除された透かし情報 w（図 8 の 8 0 3 に相当）の中から、2 次元特徴画像およびダイジェストを取り出し、後段の比較部 1 0 0 6 に出力する。このとき、取り出された 2 次元特徴画像およびダイジェストは夫々、上記原画像に対する相似画像、ハッシュ算出部 9 0 7 が計算したダイジェストである。

#### 【0 1 2 4】

次に、特徴抽出部 405 では、分離部 401 から入力される画像領域 A（本実施形態では、最下位（LSB）のビットプレーンを除く上位 7 ビットのビットプレーン 201）に対し、特徴抽出処理を行い、2 次元特徴画像を後段の比較部 1006 に出力する。

#### 【0125】

次に、ハッシュ算出部 1007 では、分離部 1001 から入力される画像領域 A のデータをハッシュ関数に入力し、ダイジェストを生成し、後段の比較部 1006 に出力する。

#### 【0126】

最後に比較部 1006 では、暗号復号部 1004 から入力される 2 次元特徴画像およびダイジェストと、特徴抽出部 405 から入力される 2 次元特徴情報およびハッシュ算出部 1007 から入力されるダイジェストを比較する。

#### 【0127】

第 1 の実施形態では、2 つの 2 次元特徴画像の間で差分がわずかである場合には、「画像内容に大きな変更がある改ざんは存在しない」旨までは伝えることが出来るが、僅かな改ざんが存在するか否かまでは判定できなかった。しかし本実施形態では 2 次元特徴画像に加え、画像領域 A に対するダイジェストも求めており、画像領域 A に 1 ビットでも変更が存在すれば、2 つのダイジェストの間で値が異なることから、これらダイジェストを比較することで僅かな改ざんでも検出することが出来る。

#### 【0128】

比較部 1006 は比較する 2 つの 2 次元特徴画像が夫々異なる場合、第 1 の実施形態と同様の結果を画像の検証者に提示する。また、夫々の 2 次元特徴画像が同一で夫々のダイジェストが同一の場合には、完全に改ざんが存在しない旨を結果として表示し、夫々の 2 次元特徴画像が同一で夫々のダイジェストが異なる場合には、検出できない（僅かな）改ざんが存在する旨を結果として表示することが可能である。

#### 【0129】

図 11 は本実施形態に係る改ざん位置検出処理の流れを示すフローチャートで

ある。図 11 を用いて、本実施形態に係る改ざん位置検出処理を順に説明する。

#### 【0130】

まずステップ S 1100 で改ざん画像の入力、及び改ざん位置検出を実行する為の種々の情報（公開鍵や誤り訂正符号のパラメータなど）を入手する。

#### 【0131】

次にステップ S 1101 で入力された改ざん画像を画像領域 A と画像領域 B に分離する。

#### 【0132】

次にステップ S 1102 で必要ならば、画像領域 B のデータに対し、ランダム化を解除するデインターリーブ処理を実行する。

#### 【0133】

そして次に、誤り訂正符号に誤り訂正可能か否かを判定する機能がある場合にはステップ S 1103 で誤り訂正が可能か否かを判定し、誤り訂正が不可能である場合はステップ S 1105 に進み、画像全体が改ざんされている旨を表示する。

#### 【0134】

ステップ S 1103 で誤り訂正が可能であると判定された場合、ステップ S 1104 に進み、誤り訂正復号処理を行い、改ざん処理により壊れた誤り訂正符号化暗号化透かし情報  $ECC'$  ( $C(w)$ ) から暗号化透かし情報  $C(w)$  を復元し、ステップ S 1106 に進む。

#### 【0135】

ステップ S 1106 では、復元された暗号化透かし情報  $C(w)$  に対し、公開鍵を用いて暗号復号処理を行い、透かし情報  $w$  を復元する。

#### 【0136】

次のステップ S 1107 では、透かし情報  $w$  中の検査ビットが一致するかを判定（検査ビットが 2 次元特徴画像のハッシュ値である場合は、透かし情報  $w$  に含まれる 2 次元特徴画像からハッシュ値を計算し、透かし情報  $w$  中の検査ビットと一致するか否かを比較）し、一致しない場合には、ステップ S 1108 に進み、正しい公開鍵で復号されていない旨、或いは正しい秘密鍵で暗号化されておら

ず画像に改ざんが施された旨を表示する。（誤り訂正符号に情報を正しく訂正可能かチェックする機能がなく、正しい誤り訂正復号が行われていない場合、ステップS1107で検査ビットが正しく復号されない。その場合には画像が改ざんされた旨だけを表示するとよい。）

ステップS1107で検査ビットが一致する場合は、ステップS1109に進む。ステップS1109では透かし情報wから2次元特徴画像とダイジェストを抽出する。次のステップS1110では、画像領域Aから2次元特徴画像とダイジェストを算出する。

#### 【0137】

次にステップS1111では、ステップS1109で透かし情報から抽出された2次元特徴画像とステップS1110で画像領域Aから算出された2次元特徴画像とを比較する。次にステップS1112では、2つの2次元特徴画像が一致しているか否かを判断し、一致していなければステップS1113に進み、図5の503～506に示すように2つの2次元特徴画像の差分画像や改ざん位置を表示して終了する。

#### 【0138】

一方、2つの2次元特徴画像が一致すれば、ステップS1114に進み、ステップS1109で透かし情報から抽出されたダイジェストとステップS1110で画像領域Aから算出されたダイジェストを比較する。ステップS1115で2つのダイジェストが一致しているか否かを判断し、一致していなければステップS1116に進み、「改ざんされているが、大きな改ざんではない」または「改ざんされているが、改ざん位置は特定できない」旨を表示し、終了する。

#### 【0139】

ステップS1115で2つのダイジェストが一致すれば、ステップS1117に進み、「画像に改ざんが行われていない」旨を画像の検証者に表示し終了する。

#### 【0140】

以上、本実施形態では、“アルゴリズム公開”かつ“秘密情報を用いずに画像の改ざん位置判定が可能”かつ“秘密情報を用いずに画像の改ざんの有無が判定



可能”である改ざん位置検出用透かし埋め込み方法および改ざん位置検出方法について詳しく述べた。

#### 【0141】

なお、第1および第2の実施形態では、図2に示すように、最下位(LSB)のビットプレーンを除く上位7ビットのビットプレーンを画像領域Aとし、最下位(LSB)のビットプレーンを画像領域Bとして説明したが、画像領域Aと画像領域Bの選択方法はその限りではない。例えば、画像領域Bは下位2ビットのビットプレーンでもよいし、入力画像中の任意のビット位置から改ざん位置検出用電子透かしの埋め込みにより画質を劣化しないように選択してもよい。そのとき画像領域Aは画像領域Bの領域でなく、かつ改ざんを検証したい画像領域のデータとするとよい。

#### 【0142】

また、第1および第2の実施形態では、入力画像として8ビットのグレースケール画像を想定したが、各画素8ビットのRGBカラー画像であってもよい。その場合、画像領域Bとして各色の最下位(LSB)のビットプレーンを用いることも可能である。

#### 【0143】

また、第1および第2の実施形態では、2次元特徴画像を1ビットからなる画像として説明したが、2次元特徴画像を暗号化、誤り訂正符号化した場合にも、透かし情報を格納できる画像領域Bが存在するなら、多ビットからなる画像であっても構わない。またそのとき、2次元特徴画像は画像領域Aよりも小さな画像である必要はなく、同じまたはそれ以上の大きさを持っていても構わない。

#### 【0144】

##### [第3の実施形態]

第1と第2の実施形態では、2次元特徴画像に基づく画像領域Aにおける改ざん位置検出方法について説明したが、第3の実施形態では誤り訂正符号化暗号化透かし情報に基づく画像領域Bにおける改ざん位置検出方法について説明する。

#### 【0145】

第3の実施形態の特徴は、透かし情報wが正しく復号された場合、暗号化透か

し情報C (w) も正しいと判断できるので、誤り訂正復号化部403で暗号化透かし情報C (w) を得る為に用いた誤りが訂正された元の誤り訂正符号化暗号化透かし情報ECC (C (w)) も正しいと判断できることを利用し、誤りが訂正された誤り訂正符号化暗号化透かし情報ECC (C (w)) と一部が破壊された誤り訂正符号化暗号化透かし情報ECC' (C (w)) とを比較し、埋め込み位置単位で改ざん位置の特定を行う点にある。

#### 【0146】

##### <改ざん位置検出用電子透かし埋め込み装置>

改ざん位置検出用電子透かし埋め込み装置については、第1もしくは第2の実施形態と同じであるので、その説明は省略する。

#### 【0147】

##### <改ざん位置検出装置>

図17は本実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。図17は図4に示した第2の実施形態に係る改ざん位置検出装置に第2改ざん位置検出部1700を加え、誤り訂正復号化部403が暗号化復号部404からの指示に従って改ざん詳細位置検出部1700に後述するデータを出力する構成となっている。なお図17において図4、10と同じ部分については同じ番号を付けている。また、図17に示した各部はハードウェアにより構成されていても良いし、各部の機能をプログラムにより表現し、コンピュータに読み込ませて実現させても良い。

#### 【0148】

以下では、図17に示す機能構成を備える改ざん位置検出装置について詳しく説明するが、第1の実施形態における改ざん位置検出装置（図4）に第2改ざん位置検出部1700を追加する構成も可能である。

#### 【0149】

図22は、改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。以下、図17のブロック図に従って、図22を用いながら、改ざん位置検出装置が行う処理を説明する。

#### 【0150】

図 2 2 において 2 2 0 1 は改竄がなされた画像を示し、2 2 1 0 の領域（網掛けされた三日月の形状の領域）が改竄がなされた領域を示す。以下の説明では 2 2 0 1 に示す改竄画像を例に取り説明するが、各種の改竄画像に対しても以下説明する処理は適用可能である。

#### 【0 1 5 1】

改ざん画像 2 2 0 1（入力画像）は、改ざん位置の検証の為、分離部 4 0 1 に入力される。分離部 4 0 1 では入力画像を画像領域 A と改ざん位置検出用の透かし情報が埋め込まれている画像領域 B に分離する。本実施形態でも上記実施形態と同様に、図 2 に示すように画像領域 A は最下位（LSB）のビットプレーンを除く上位 7 ビットのビットプレーン 2 0 1 とし、画像領域 B は LSB のビットプレーン 2 0 2 とする。既に述べたように画像領域 B には改ざん位置検出用の透かし情報が埋め込まれている。

#### 【0 1 5 2】

このとき画像領域 B から得られる画像は画像の改ざんにより、図 5 の 5 0 2 で示したように、改ざん位置 5 2 0 で破壊されている可能性がある。

#### 【0 1 5 3】

次に、分離部 4 0 1 で分離された画像領域 B のデータは、デインターリーバ 4 0 2 に入力される。デインターリーバ 4 0 2 では、一部が壊れたランダム化された誤り訂正符号化暗号化透かし情報  $S' (ECC(C(w)))$  を構成する各ビット列の並びを、を元のビットの並びに戻す処理を行う。

#### 【0 1 5 4】

そしてデインターリーバ 4 0 2 は、デインターリーブ処理を施した一部が壊れた誤り訂正符号化暗号化透かし情報、即ち  $ECC'(C(w))$  を生成し、後段の誤り訂正復号化部 4 0 3 に出力する。

#### 【0 1 5 5】

図 2 2 に示す 2 2 0 2 は、図 5 の 5 0 2 で示した画像領域 B に対してデインターリーブ処理を施して得られる、一部が破壊された誤り訂正符号化暗号化透かし情報  $ECC'(C(w))$  を 2 次元画像として表現したものである。改ざんによって破壊されたビット情報は画像 2 2 0 2 全体に広がっている。

## 【0 1 5 6】

なお、誤り訂正符号の種類によっては、埋め込み時にインターリーブを必要としない場合がある。従って、デインターリーブ 4 0 2 におけるデインターリーブ処理は必須ではなく、改ざん位置検出用電子透かしの埋め込み時にインターリーブ 1 0 5 で ECC (C (w)) にインターリーブ処理を施した場合にのみデインターリーブ処理が必要となる。

## 【0 1 5 7】

誤り訂正復号化部 4 0 3 では入力された一部が破壊された ECC' (C (w)) に対して誤り訂正復号処理を行い、暗号化透かし情報 C (w) を後段の暗号復号部 4 0 4 に出力する。

## 【0 1 5 8】

ここで、画像領域 B の透かしデータが改ざんにより大きく破壊され、誤り訂正符号化暗号化透かし情報 ECC' (C (w)) が正しく誤り訂正復号が出来ない場合、「改ざん位置の特定はできないが、画像全体が改ざんされている」旨を結果として表示し、処理を中止する（但し、誤り訂正符号自体に正しく誤り訂正復号できないことを伝える機能を持っている必要がある）。

## 【0 1 5 9】

一般に誤り訂正復号化部 4 0 3 は、誤り訂正符号化時に用いた規則を利用して、一部が破壊された誤り訂正符号化暗号化透かし情報 ECC' (C (w)) の誤りを訂正し、誤りが訂正された誤り訂正符号化暗号化透かし情報 ECC (C (w)) を生成する。そして、誤りが訂正された誤り訂正符号化暗号化透かし情報 ECC (C (w)) から元の情報である暗号化透かし情報 C (w) を取り出す処理を行う。

## 【0 1 6 0】

図 2 2 の 2 2 0 3 は 2 2 0 2 で示した一部が破壊された誤り訂正符号化暗号化透かし情報 ECC' (C (w)) の誤りを訂正した、誤り訂正符号化暗号化透かし情報 ECC (C (w)) を 2 次元画像として表現したものである。

## 【0 1 6 1】

本実施形態では、誤り訂正復号化部 4 0 3 は、誤り訂正復号した暗号化透かし

情報  $C(w)$  を後段の暗号復号部 4 0 4 に出力した後も、一部が破壊された誤り訂正符号化暗号化透かし情報  $ECC'(C(w))$  と誤りが訂正された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  を保持するとする。

#### 【0162】

そして本実施形態では、誤り訂正復号化部 4 0 3 は、暗号復号部 4 0 4 から制御信号を受けると、一部が破壊された誤り訂正符号化暗号化透かし情報  $ECC'(C(w))$  と誤りが訂正された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  を後段の第 2 改ざん位置検出部 1 7 0 0 に出力する構成をとるとする。

次に暗号復号部 4 0 4 では、入力された誤り訂正復号された暗号化透かし情報  $C(w)$  を復号し、透かし情報  $w$  を復元する。公開鍵暗号方式で暗号化透かし情報  $C(w)$  が暗号化されている場合、暗号化に用いた秘密鍵に対応する公開鍵を入手し、公開鍵を用いて復号処理を行う。

#### 【0163】

このとき、第 1 と第 2 の実施形態と同様、本実施形態においても、暗号復号部 4 0 4 で透かし情報  $w$  が正しいか検証を行うが、本実施形態では、透かし情報  $w$  全体が正しいか検証を行う。従って、検査ビットは透かし情報の一部に対して整合性の検証を行う為の検査ビットではなく、検査ビット自身を除く透かし情報  $w$  の全てに対して整合性の検証を行う為の検査ビットであるとする。

#### 【0164】

既に第 1、第 2 の実施形態でも検査ビットを用いた透かし情報  $w$  の整合性の検証方法を説明したが、基本的な検証方法は本実施形態においても同様である。即ち、検査ビットが検査ビットを除く透かし情報のハッシュ値である場合、検査ビットを除く透かし情報をハッシュ関数に入力して得られるハッシュ値を、透かし情報の一部である検査ビットの値と比較することで、透かし情報全体の整合性を検証することが出来る。

#### 【0165】

改ざん位置検出用電子透かし埋め込み装置の暗号化部 9 0 3 において、ブロック暗号方式（ブロック単位で暗号化を実行する暗号方式）を用いて透かし情報を

暗号化する場合、一般に透かし情報 $w$ はまずブロック単位（鍵長の単位）に分割され、その後ブロック単位で暗号化される。しかし、分割されたブロックが鍵長に満たない単位の情報量である場合、所定の値（例えばを 0）をパディングし、暗号化処理を行う。例えば、公開鍵暗号方式の一種である R S A 暗号方式もブロック暗号に分類され、ブロック単位で暗号化処理を行う。

#### 【0 1 6 6】

このような場合、透かし情報 $w$ にパディング値を加えて生成された暗号化透かし情報 $C(w)$ が正しいことを検証するには、透かし情報 $w$ の暗号化時に加えたパディング値についても整合性が取れているか、暗号復号時にチェックする必要がある。その場合、パディング値も透かし情報 $w$ と同様に扱うとよい。即ち、改ざん位置検出用電子透かし埋め込み装置では、検査ビットは、検査ビット自身を除く透かし情報とパディング値に対するハッシュ値またはチェックサムとし、改ざん位置検出装置の暗号復号部 4 0 4 では検査ビット自身を除く透かし情報とパディング値から算出される検査ビットの値と透かし情報中の検査ビットの値を比較し、透かし情報の整合性を検証すればよい。

#### 【0 1 6 7】

以降、説明を簡単にする為、パディング値が存在する場合の処理については説明を省略する。

#### 【0 1 6 8】

一般に暗号技術は解読を困難にする為、入力データの僅かな変化に対し、出力データはランダムに変化するように設計されており、鍵情報がなければその入出力データの対応関係を推測することは困難である。従って、本実施形態においても、透かし情報と検査ビットの整合性を維持させつつ、偽の暗号化透かし情報を意図的に作成することは、暗号化に用いた秘密の鍵（公開鍵暗号方式では秘密鍵、共通鍵暗号方式では共通鍵）の知識なしには非常に困難である。

#### 【0 1 6 9】

従って、暗号化に用いる暗号方式の安全性が保証されていれば、透かし情報 $w$ と検査ビットの間で整合が取れていないならば、暗号化透かし情報 $C(w)$ に改ざんが行われたとみなし、透かし情報 $w$ と検査ビットの間で整合が取れているな

らば、暗号化透かし情報  $C(w)$  に改ざんは行われていないと見なす判断を行っても、実用上差し支えないと言える。

#### 【0 1 7 0】

本実施形態では、透かし情報  $w$  が整合性を満たしていれば、暗号化透かし情報  $C(w)$ 、そして暗号化透かし情報  $C(w)$  を得る為に用いた誤りが訂正された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  も正しいと見なす。従って、検証者は秘密の鍵を入手することなく、埋め込みに用いた誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  を知ることが出来る。

#### 【0 1 7 1】

第 1 と第 2 の実施形態では誤り訂正復号化部 4 0 3 は正しい暗号化透かし情報  $C(w)$  を出力するとして簡単に説明を行ったが、実際には誤り訂正復号化部 4 0 3 から出力される暗号化透かし情報は必ずしも元の正しい暗号化透かし情報  $C(w)$  と同一であるとは限らない。

#### 【0 1 7 2】

例えば、誤り訂正符号化部 1 0 4 が符号化処理を行う際に用いるパラメータは公開されている為、このパラメータを用いて偽造者が誤り訂正復号化部 4 0 3 で誤り訂正復号可能なように、偽の暗号化透かし情報を誤り訂正符号化し、偽の誤り訂正符号化暗号化透かし情報を生成して、画像領域 B と置き換えた場合を想定してみる。このとき、改ざん位置検出装置の誤り訂正復号化部 4 0 3 は、単純に誤り訂正復号を行い、偽の暗号化透かし情報を出力する。

#### 【0 1 7 3】

また、何らかの改ざんを行った結果、偶然に、誤った暗号化透かし情報  $C'(w)$  の誤り訂正符号化情報に相当する誤り訂正符号化暗号化透かし情報  $ECC(C'(w))$  が生成される場合もあり得る。

#### 【0 1 7 4】

また誤り訂正符号自体に誤り訂正可能か検出する機能がない場合、誤り訂正復号部 4 0 3 は、入力される情報を単純に規則に基づいて誤り訂正復号化し、本来の暗号化透かし情報  $C(w)$  とは全く異なる暗号化透かし情報  $C'(w)$  を出力する場合もある。

**【0 1 7 5】**

上述のように誤り訂正復号化部 4 0 3 から、誤った暗号化透かし情報 C' (w) が出力される様々なケースが想定される。

**【0 1 7 6】**

しかし、本実施形態では、暗号復号部 4 0 4 で暗号化透かし情報を復号後、検査ビットを用いて透かし情報の整合性を検証することで、透かし情報の改ざんを検出することが出来る。

**【0 1 7 7】**

例えば、検査ビットが検査ビットを除く透かし情報のハッシュ値である場合、暗号復号部 4 0 4 では、検査ビットを除く透かし情報をハッシュ関数に入力して得られるハッシュ値を、透かし情報の一部である検査ビットの値と比較し、一致しない場合には、透かし情報、暗号化透かし情報が誤っている、即ち改ざんが加えられていると見なすことが出来る。その場合、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

**【0 1 7 8】**

また、第 1 と第 2 の実施形態で述べたように、暗号化透かし情報 C (w) が本来暗号化（署名生成）に用いられるべき秘密鍵（例えば、秘密鍵 p r i 1）と異なる秘密鍵（例えば、秘密鍵 p r i 2）で暗号化されている場合、本来用いられるべき秘密鍵（秘密鍵 p r i 1）に対応する公開鍵（公開鍵 p u b 1）を用いて暗号復号を行っても、正しく復号されない。従って、検査ビットを用いて透かし情報の整合性を検証しても、透かし情報の誤りが検出される。この場合も、同様に改ざんが加えられているとし、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

**【0 1 7 9】**

また、誤って、暗号化（署名生成）に用いた秘密鍵に対応していない公開鍵を用い、透かし情報 w の暗号化を復号した場合にも検査ビットの値は一致しない。この場合、「暗号化透かし情報の復号に用いる鍵が異なる」旨を画像の検証者に



通知しても良い。但し、一般に画像の検証者は暗号化の復号の為の鍵を間違わないように注意すべきであり、暗号復号部 4 0 4 においても暗号化透かし情報の復号に用いる鍵が誤っていると特定できない場合は、画像に改ざんが加えられていると見なし、改ざん位置は特定できないが画像が改ざんされている旨、或いは改ざんが画像全体に渡っているとして、画像全体が改ざんされている旨を表示してもよい。

#### 【0 1 8 0】

暗号復号部 4 0 4 の内部処理において、検査ビットを用いた透かし情報の検証の結果、透かし情報中の検査ビットの値が、検査ビットを除く他の透かし情報から算出される検査ビット（例えばハッシュ値やチェックサム）と一致するならば、暗号復号部 4 0 4 は、誤り訂正復号部 4 0 3 に対し制御信号を送る。

#### 【0 1 8 1】

誤り訂正復号化部 4 0 3 は、暗号復号部 4 0 4 からの制御信号を受け、一部が破壊された誤り訂正符号化暗号化透かし情報  $EC C'$  ( $C(w)$ ) と誤りが訂正された誤り訂正暗号化透かし情報  $EC C$  ( $C(w)$ ) を後段の第 2 改ざん位置検出部 1 7 0 0 に出力する。

#### 【0 1 8 2】

従って、本実施形態では、誤り訂正復号化部 4 0 3 で単純に誤り訂正復号が成功しても、第 2 改ざん位置検出部 1 7 0 0 は改ざん位置の検出を行わない。

#### 【0 1 8 3】

これは、既に述べたように、誤り訂正復号化部 4 0 3 で誤り訂正復号が成功しても、誤り訂正復号化部 4 0 3 から必ずしも正しい暗号化透かし情報  $C(w)$  が出力されとは限らず、誤った暗号化透かし情報  $C'(w)$  が出力される可能性もある。従って、誤り訂正復号化部 4 0 3 からの出力データは信頼性が低く、そのデータを元にした改ざん位置検出は信頼性が低いと考えられる為である。

#### 【0 1 8 4】

一方、秘密の鍵（公開鍵暗号方式における秘密鍵、または共通鍵暗号方式における共通鍵）の知識なしに透かし情報  $w$  の整合性を満たす形で改ざんを行うことは暗号の原理上非常に困難である。従って、透かし情報  $w$  の整合性を検証できれ

ば、暗号化透かし情報  $C(w)$  は信頼のできるデータであり、信頼のできる暗号化透かし情報  $C(w)$  を再誤り訂正符号化して得られる誤りが訂正された誤り訂正符号化暗号化透かし情報  $EC C(C(w))$  も信頼できると考えられる。

#### 【0185】

従って、透かし情報  $w$  の整合性を検証した上で、誤りが訂正された誤り訂正符号化暗号化透かし情報  $EC C(C(w))$  と一部を破壊された誤り訂正符号化暗号化透かし情報  $EC C'(C(w))$  を比較すれば、正確で誤りのない改ざん位置の特定が可能になると考えられる。

#### 【0186】

次に、暗号復号部 404 は暗号化が解除された透かし情報  $w$ （例えば、図 8 の 803 に相当）の中から、2次元特徴画像およびダイジェストを取り出し、後段の比較部 1006 に出力する。このとき、取り出された2次元特徴画像およびダイジェストは夫々、上記原画像に対する相似画像、ハッシュ算出部 907 が計算したダイジェストである。

#### 【0187】

以降、特徴抽出部 405、ハッシュ算出部 1007、比較部 1006 の動作は、第 2 の実施形態の動作と同じである。

#### 【0188】

次に、特徴抽出部 405 では、分離部 401 から入力される画像領域  $A$ （本実施形態では、最下位（LSB）のビットプレーンを除く上位 7 ビットのビットプレーン 201）に対し、特徴抽出処理を行い、2次元特徴画像を後段の比較部 1006 に出力する。

#### 【0189】

次に、ハッシュ算出部 1007 では、分離部 401 から入力される画像領域  $A$  のデータをハッシュ関数に入力し、ダイジェストを生成し、後段の比較部 1006 に出力する。

#### 【0190】

比較部 1006 では、暗号復号部 404 から入力される2次元特徴画像およびダイジェストと、特徴抽出部 405 から入力される2次元特徴情報およびハッシ

ユ算出部 1007 から入力されるダイジェストを比較する。

#### 【0191】

比較部 1006 は、比較する 2 つの 2 次元特徴画像が夫々異なる場合、第 1 の実施形態と同様の結果を画像の検証者に提示する。また、夫々の 2 次元特徴画像が同一で夫々のダイジェストが同一の場合には、画像領域 A には、完全に改ざんが存在しない旨を結果として表示し、夫々の 2 次元特徴画像が同一で夫々のダイジェストが異なる場合には、画像領域 A に位置を検出できない（僅かな）改ざんが存在する旨を結果として表示することが可能である。

#### 【0192】

本実施形態では、更に第 2 改ざん位置検出部 1700 を用い、第 1、第 2 の実施形態で述べた画像領域 A における改ざん位置検出に加え、画像領域 B における改ざん位置検出を実現するが、以下、第 2 改ざん位置検出部について詳しく説明する。

#### 【0193】

図 18 は第 2 改ざん位置検出部 1700 の機能構成を示すブロック図である。第 2 改ざん位置検出部 1700 は、第 2 比較部 1801、インターリーバ 1802、埋め込み位置対応部 1803 から成り立っている。以下、各ブロックについて説明する。

#### 【0194】

第 2 比較部 1801 には、誤り訂正復号化部 403 から、誤りが訂正された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  と一部が破壊された誤り訂正符号化暗号化透かし情報  $ECC'(C(w))$  が入力される。

#### 【0195】

既に述べたが、透かし情報  $w$  の整合性が既に検証されている為、暗号化透かし情報  $C(w)$  と誤りが訂正された誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  は、それぞれ、改ざん位置検出用電子透かし埋め込み装置で生成した暗号化透かし情報  $C(w)$  と誤り訂正符号化暗号化透かし情報  $ECC(C(w))$  と全く同一であると見なす。

#### 【0196】

第2比較部1801では、入力された2つのビット系列、即ち、一部が破壊された誤り訂正符号化暗号化透かし情報 $ECC'(C(w))$ と誤りが訂正された誤り訂正符号化暗号化透かし情報 $ECC(C(w))$ をビット単位で比較する。

#### 【0197】

2つのビット系列が1または0のビットからなる場合、2つのビット系列の簡単な比較は、2つのビット系列で夫々同位置に位置するビット同士のXOR（排他的論理和）値を算出することで実現できる。2つのビット系列で夫々同位置に位置するビット同士の値が同じであればXOR値は0、異なればXOR値は1となる。このようにして、2つのビット系列で対応するビット同士のXOR値を並べたビット系列（第2改ざん位置特定ビット系列BS）を求め、後段のインターリーバ1803に出力する。ここで第2改ざん位置特定ビット系列BSは一般には、2つのビット系列で互いに異なるビット値であるビットの位置を示すものである。

#### 【0198】

図22の2204は第2改ざん位置特定ビット系列BSを2次元画像として表現したもので、図22の2202で示される一部が破壊された誤り訂正符号化暗号化透かし情報と2203で示される誤りが訂正された誤り訂正符号化暗号化透かし情報とで、異なるビット値の分布（位置）を示している。2204では、改ざんによって破壊されたビットが画像全体に分散して存在している。

#### 【0199】

次にインターリーバ1802は、入力された第2改ざん位置特定ビット系列BSの並びを並び替え、インターリーブ処理を施した第2改ざん位置特定ビット系列S（BS）を生成し、後段の埋め込み位置対応部1803に出力する。

#### 【0200】

このときインターリーバ1802が行う処理は、改ざん位置検出用電子透かし埋め込み装置におけるインターリーバ105と同一の処理である。既に述べているがインターリーバ1802は必須の処理ではなく、改ざん位置検出用電子透かし埋め込み装置でインターリーバを用いた場合にのみ必要となる処理である。

#### 【0201】

次に埋め込み位置対応部 1803 では、インターリーブ処理を施した第 2 改ざん位置特定ビット系列 S (BS) と入力画像 (改ざん画像) における埋め込み位置を対応付ける。

#### 【0202】

図 23 は、第 2 改ざん位置特定ビット系列 S (BS) と改ざん画像との対応を示す図である。一次元配列のビット列である第 2 改ざん位置特定ビット系列 S (BS) を 2 次元配列に並べることで、同図左の 2 次元ビット配列 2300 が得られる。即ち、改ざん画像 2201 のサイズが縦 H 画素、横 W 画素であるとする、第 2 改ざん位置特定ビット系列 S (BS) も同様に先頭ビットから順番に並べて縦 H 画素、横 W 画素に配列させることで、2 次元ビット配列 2300 を得ることができる。このような 2 次元ビット配列 2300 を生成することで、同図右に示した改ざん画像 2201 において改ざん領域 2210 に対応する領域 2301 にビット値 "1" が、その他の領域にはビット値 "0" が配置されることになる。よって、2 次元ビット配列 2300 においてビット値が 1 であるビット位置に対応する改ざん画像 2201 における画素を参照することで、この参照した画素の集合が改ざん領域 (2210) となる。

#### 【0203】

図 22 の 2205 はインターリーブ処理を施した第 2 改ざん位置特定ビット系列 S (BS) において、改ざん領域 2210 を明示的に示した図である。2204 では改ざんによって破壊されたビットが画像全体に分散して存在していたが、2205 では、改ざんによって破壊されたビットが改ざん領域 2210 に集中して存在している。

#### 【0204】

第 2 改ざん位置検出部 1700 は、最後に改ざん位置を表示して終了する。このとき、第 1 や第 2 の実施形態で既に述べたように改ざん位置を示す差分画像 (例えば画像 2205) を表示してもよいし、図 22 の画像 2206 で示すように入力画像に対して差分画像 (例えば画像 2205) をオーバーレイ (重ね合わせ) して改ざん位置を表示しても良い。

#### 【0205】

2次元特徴画像の解像度（画像の大きさ）が改ざん画像の解像度よりも低い場合、本実施形態における改ざん位置検出結果（図22の画像2206）の方が第1、第2の実施形態における改ざん位置検出結果（図5の画像506）よりも高い解像度（埋め込み位置単位）で改ざん位置の特定を実現していることが分かる。

#### 【0206】

以上、デインターリーブ処理を施した一部が破壊された誤り訂正符号化暗号化透かし情報 $ECC'(C(w))$ と誤りが訂正された誤り訂正符号化暗号化透かし情報 $ECC(C(w))$ を比較し、改ざん位置を特定する第2改ざん位置検出部1700の処理について詳しく述べた。

#### 【0207】

なお、本実施形態では、誤り訂正復号化部403が、誤りが訂正された誤り訂正暗号化透かし情報 $ECC(C(w))$ を生成するとして説明を行ったが、誤り訂正復号化部403が、暗号化透かし情報 $C(w)$ のみを出力し、誤りが訂正された誤り訂正暗号化透かし情報 $ECC(C(w))$ を外部に出力しない構成をとる場合、誤り訂正復号化部403から出力される暗号化透かし情報 $C(w)$ を再び誤り訂正符号化し、誤りが訂正された誤り訂正暗号化透かし情報 $ECC(C(w))$ を生成する構成をとってもよい。

#### 【0208】

透かし情報 $w$ が整合性を満たす場合、暗号化透かし情報 $C(w)$ もそれを誤り訂正符号化した誤り訂正符号化暗号化透かし情報 $ECC(C(w))$ も正しいと見なすことが出来る。

#### 【0209】

暗号化透かし情報 $C(w)$ を再び誤り訂正符号化した誤り訂正暗号化透かし情報 $ECC(C(w))$ と一部が破壊された誤り訂正符号化暗号化透かし情報 $ECC(C(w))$ と比較することで、同様に正確に改ざん位置を特定することが可能である。

#### 【0210】

図19は本実施形態に係る改ざん位置検出処理の流れを示すフローチャートで

ある。図 20 は図 19 のステップ A1（ステップ S1910）の詳細を示すフローチャートで、図 21 は図 19 のステップ A2（ステップ S1920）の詳細を示すフローチャートである。

#### 【0211】

以下、図 19、図 20、図 21 を用いて、本実施形態に係る改ざん位置検出処理について説明する。なお、図 19、図 20 中で図 11 と同じ番号が記された処理は、図 11 と同様の処理を行うとする。

#### 【0212】

ステップ S1100～ステップ S1106 の処理は、第 1、第 2 の実施形態で詳しく述べたのでここでの説明は省略する。

#### 【0213】

ステップ S1107 では、透かし情報 w 中の検査ビットを用いて、透かし情報 w の整合性を検証する。ステップ S1107 で検査ビットが一致しない場合（透かし情報 w が整合性を満たさない場合）には、ステップ S1108 に進み、画像に改ざんが施された旨、あるいは、暗号化（署名生成）で用いた秘密鍵と復号で用いた公開鍵が対応していない旨を表示する。

#### 【0214】

ステップ S1107 で検査ビットが一致する場合は、ステップ A1（ステップ S1910）に進む。ステップ A1（ステップ S1910）における処理の詳細は、図 11 のステップ S1109～ステップ S1117 と同様の処理であり、第 2 の実施形態で詳しく説明を行った為、説明を省略する。

#### 【0215】

次に、ステップ A1（ステップ S1910）の処理が終了した後、ステップ A2（ステップ S1920）に移る。ステップ A2（ステップ S1920）では、図 17 の第 2 改ざん位置検出部 1700 における処理が行われる。

#### 【0216】

既にステップ S1107 で透かし情報 w 及び暗号化透かし情報 C（w）の整合性が確認されているので、ステップ S2101 の制御信号送信処理では、暗号復号部 404 から誤り訂正復号化部 403 に制御信号を送る。

**【0 2 1 7】**

誤り訂正復号化部 4 0 3 はこの制御信号を受けて、後段の第 2 改ざん位置検出部 1 7 0 0 に一部が破壊された誤り訂正符号化暗号化透かし情報 E C C' (C (w)) と誤りが訂正された誤り訂正符号化暗号化透かし情報 E C C (C (w)) を出力する。

**【0 2 1 8】**

次に、ステップ S 2 1 0 2 の比較処理では、既にステップ S 1 1 0 2 でインターリーブ処理された一部が破壊された誤り訂正符号化透かし情報 E C C' (C (w)) のビット系列とステップ S 1 1 0 4 で誤りが訂正された誤り訂正符号化暗号化透かし情報 E C C (C (w)) のビット系列とを比較し、上記第 2 改ざん位置特定ビット系列 B S を生成する。

**【0 2 1 9】**

次に、ステップ S 2 1 0 3 では、2 つのビット系列が一致するか否かを判定する。一致した場合（例えば、2 つのビット系列において位置的に対応するビット同士の X O R 値を、全てのビット同士について求め、全ての X O R 値が 0 である場合）、ステップ S 2 1 0 7 に進み、画像領域 B に改ざんが存在しない旨を表示し、改ざん位置検出装置の処理を終了する。

**【0 2 2 0】**

一致しない場合（例えば、2 つのビット系列において位置的に対応するビット同士の X O R 値を、全てのビット同士について求め、1 である X O R 値が 1 つ以上存在する場合）、ステップ S 2 1 0 4 に進む。

**【0 2 2 1】**

次にステップ S 2 1 0 4 では、第 2 改ざん位置特定ビット系列 B S に対し、ビット系列の並びを並べ替えるインターリーブ処理を実行し、インターリーブ処理が施された第 2 改ざん位置特定ビット系列 S (B S) を生成する。

**【0 2 2 2】**

なお、ステップ S 2 1 0 4 のインターリーブ処理は、改ざん位置検出用電子透かし埋め込み装置においてインターリーバ 1 0 5 が存在し、誤り訂正符号化暗号化透かし情報 E C C (C (w)) に対しインターリーブ処理を行ったときにのみ



必要となる。

#### 【0223】

次に、ステップS2105では、インターリーブ処理が施された第2改ざん位置特定ビット系列S(BS)のビットと入力画像中の位置を対応付ける位置対応処理を行う。

#### 【0224】

次に、ステップS2106では、入力画像中の位置と対応付け、改ざん位置の表示を行う。このとき、第1や第2の実施形態で述べたように改ざん位置を入力画像にオーバーレイ（重ね合わせ）して表示してもよいし、その表示方法については限定するものではない。

#### 【0225】

ステップS2106の処理が終了したら、改ざん位置検出装置の処理を終了する。

#### 【0226】

なお、図19ではステップA1、ステップA2の順序で処理を行う場合について説明したが、ステップA1とステップA2の処理の順序が逆転していてもよく、ステップA2、ステップA1の順序で処理を行っても構わない。

#### 【0227】

また、上記ステップA1、A2のステップS1113、S1116、S117、S2107、S2106の各ステップにおける処理は、本実施形態では夫々で独自に実行されていたが、まとめて総合的な結果を通知しても良い。

#### 【0228】

例えば、ステップS1113で特定した（2次元特徴画像から求まる）改ざん位置を用いて画像全体の改ざんの概要を示し、ステップS2106で特定した（第2改ざん位置特定ビット系列BSから求まる）改ざん位置を用いて正確な改ざん位置を示してもよい。また、ステップS1113で特定した画像領域Aの改ざん位置とステップS2106で特定した画像領域Bの改ざん位置を統合して表示しても良い。

#### 【0229】

第 1 および第 2 の実施形態では、2 次元特徴画像に基づいて改ざん位置の検出を行う為、2 次元特徴画像が入力画像の縦横の解像度よりも小さい場合、改ざん位置の特定は 2 次元特徴画像の解像度で行っていた。また改ざん位置の特定は画像領域 A を対象とし、画像領域 B を対象としていなかった。

#### 【0 2 3 0】

しかし、本実施形態に係る上記方法を用いれば、2 次元特徴画像の解像度に関わらず、画像領域 B における埋め込み位置単位の正確な改ざん位置検出が可能である。

#### 【0 2 3 1】

従って、第 3 の実施形態では、第 1 と第 2 の実施形態で実現した

- (1) 2 次元特徴画像を用いた画像領域 A におけるロバストな改ざん位置検出
  - (2) ダイジェストを用いた画像領域 A における改ざん有無検出
- に加え、
- (3) 画像領域 B における埋め込み位置単位の改ざん位置検出
- を実現することが可能となる。

#### 【0 2 3 2】

なお、本実施形態では、8 ビットグレースケール画像の L S B に改ざん位置検出用の透かしデータを埋め込む場合を例に説明を行ったが、改ざん位置検出用の透かしデータの埋め込みは、L S B に限らない。

#### 【0 2 3 3】

第 7 や第 8 の実施形態でも説明するが、圧縮符号化画像の代表である J P E G 圧縮符号化画像や J P E G 2 0 0 0 圧縮符号化画像などにおいても適用可能である。

#### 【0 2 3 4】

例えば、J P E G 圧縮符号化画像や J P E G 2 0 0 0 圧縮符号化画像における量子化後の離散コサイン変換 (D C T) 係数や離散ウェーブレット変換 (D W T) 係数に対し、例えば、量子化後の係数が所定の定数の奇数倍または偶数倍となるように量子化することで、0 または 1 のビット情報を埋め込むことが可能であ

る。例えばある係数の値が5の場合、この係数に” 1 ”を埋め込みたい場合には商が奇数となるような量子化値（第1の量子化値）を用いればよいし、この係数に” 0 ”を埋め込みたい場合には商が偶数となるような量子化値（第2の量子化値）を用いればよい。このような第1の量子化値、第2の量子化値の例としては共に” 2 ”が代表的ではあるが、夫々の量子化値で異なる値を用いても良い。

#### 【0 2 3 5】

このように画像の周波数係数に改ざん位置検出用透かし情報を埋め込む場合、改ざん位置検出装置では、量子化後の周波数係数に基づいた改ざん位置の検出を実現することが出来る。

#### 【0 2 3 6】

また本実施形態で述べた改ざん位置検出装置の特徴は、透かし情報の整合性が確認できれば画像領域Bの改ざん位置を検出できることから、透かし情報として画像とは関係のない情報を用いてもよい。

#### 【0 2 3 7】

例えば、予め決められた情報とその情報の検査ビットから透かし情報を構成してもよい。透かし情報としては、改ざん位置検出システム全体で予め決めておいた固定の情報などが考えられる。改ざん位置検出装置の利用者は、暗号復号部で、抽出された透かし情報が予め決められた情報と一致するかを確認し、かつ透かし情報の整合性を確認すれば、透かし情報が改ざんされていないことを確認できる。透かし情報には、特徴画像情報や画像領域Aのハッシュ値が含まれないため、図19のステップA1の処理は省略されるが、ステップA2の処理を実行することで画像領域Bの改ざん位置検出は可能であり、このような変形例も改ざん位置検出装置として十分に機能する。

#### 【0 2 3 8】

透かし情報の情報量が少なければ、画像領域Bに収まるように暗号化透かし情報に対して冗長な誤り訂正符号化を行うことが出来る。従って、画像の多くの部分が改ざんされた場合にも、誤り訂正復号が可能となり、改ざんに対する耐性、即ち改ざん位置の特定能力を強めることが出来る。

#### 【0 2 3 9】

#### [第 4 の実施形態]

第 1 乃至 3 の実施形態では、主に 2 次元特徴画像が各画素 1 ビットの場合について説明してきた。しかし画像の種類によっては、各画素 1 ビットの高精細画像（画素数が大きい画像）よりも各画素 8 ビットなどの多階調画像の方が原画像の雰囲気をよく表すことが出来る場合もある。本実施形態では、特徴抽出部の処理で多階調の画像を生成するようにしてもよい。

##### 【0 2 4 0】

例えば、第 1 の実施形態では、特徴抽出部は縦 2 5 6 画素、横 2 5 6 画素の各画素 1 ビットの 2 次元特徴画像を生成したが、本実施形態では、縦 1 2 8 画素、横 1 2 8 画素の各画素 4 ビットを生成してもよい。このとき透かし情報のデータ量は両者で同一である。

##### 【0 2 4 1】

多階調の 2 次元特徴画像に対応する場合には、透かし情報 w の内部に図 8 の 8 0 4 に示すような 2 次元特徴画像の「階調数」を記録する領域を導入し、2 次元特徴画像のデータの並びを定義しておけば、透かし情報から多階調の 2 次元特徴画像を復元することが可能である。また図示しないが 2 次元特徴画像を構成する「色情報」なども透かし情報の一部として導入可能である。従って、透かし情報のフォーマットは世間でよく用いられる画像フォーマット（例えば T I F F や J P E G など）と類似の構成をとることが出来る。

##### 【0 2 4 2】

多値の 2 次元特徴画像を生成する為の処理の一例としては、入力画像に対する縮小処理、離散ウェーブレット変換処理後に低周波成分を取得する処理など、様々な処理が可能である。既に述べたが、特徴抽出処理は透かし情報の中の特徴抽出処理 I D に記載しておけば、改竄位置検出装置は改ざん画像から抽出される透かし情報 w 中の特徴抽出処理 I D を元に特徴抽出部で行う特徴抽出処理を知ることが出来る。その為、改ざん位置検出装置の特徴抽出部で特徴抽出処理 I D に基づく特徴抽出を実行することで、改ざん位置検出が可能になる。

##### 【0 2 4 3】

#### [第 5 の実施形態]

第 5 の実施形態では、2 次元特徴画像のデータ量削減方法について述べる。画像から改ざん位置検出を行う場合、特定の関心領域以外に改ざんが行われていたとしても検出する必要が無い場合もある。例えば、車の画像中で車のナンバープレートの領域しか興味がなく、画像中でナンバープレートの領域に対する改竄の有無や位置の検出のみを行う場合がある。

#### 【0 2 4 4】

この場合、画像全体の情報から 2 次元特徴画像を計算し、計算した 2 次元特徴画像全部を透かし情報  $w$  内部に配置すると情報量に無駄がある。そのような場合、2 次元特徴画像中で最も重要な領域を切り取り、切り取った部分の画像（部分画像）を 2 次元特徴画像として、透かし情報  $w$  内部に配置するとよい。その場合、図示しないが、元の 2 次元特徴画像の左上隅を原点とする座標において、部分画像の左上隅の座標（ $a_1$ 、 $a_2$ ）から縦  $p_x$ 、横  $p_y$ （部分画像の縦のサイズが  $P_x$ 、横のサイズが  $P_y$  とする）の画像を各画素 8 ビットで切り出しているという情報を記録できるように透かし情報のフォーマットを形成すればよい。

#### 【0 2 4 5】

例えば、デジタルカメラで撮影する画像に自動的に透かし情報を埋め込む場合、フォーカスが合った位置を中心とする所定の矩形領域を上記部分画像としておくだけで、透かし情報  $w$  内の 2 次元特徴画像のデータ量を大幅に削減することが出来る。

#### 【0 2 4 6】

更には、2 次元特徴画像は画像データである為、得られた 2 次元特徴画像に対し、様々な圧縮処理を施し、圧縮した 2 次元特徴画像を透かし情報  $w$  内に配置することも可能である。

#### 【0 2 4 7】

上記で述べた 2 次元特徴画像の抽出処理は特徴抽出処理 ID として、透かし情報  $w$  内に記録することで、改ざん位置検出時にも同様の 2 次元特徴画像を生成することが出来る。

#### 【0 2 4 8】

[第 6 の実施形態]

第 1 ～ 第 5 の実施形態では、特徴抽出部では単一の特徴抽出処理を用いて、2 次元特徴画像を生成する処理について述べたが、第 6 の実施形態では、特徴抽出部では複数の特徴抽出処理を用いて複数の 2 次元特徴画像を生成する。

#### 【 0 2 4 9 】

特徴抽出部で単一の特徴抽出処理を行い 2 次元特徴画像を生成する場合、改ざんの前後における 2 次元特徴画像に差がない場合には改ざん位置まで検出することが難しかった。

#### 【 0 2 5 0 】

しかし、複数の特徴抽出処理を行えば、いずれかの特徴抽出処理で生成される 2 次元特徴画像において改ざんの前後で差が発生するならば、改ざん位置の検出が可能になる。

#### 【 0 2 5 1 】

本実施形態では、複数の特徴抽出処理から得られる複数の 2 次元特徴画像を埋め込み装置と改竄位置検出装置の双方で求め、同じ抽出処理を用いて得られた画像同士を比較することで、第 1 ～ 第 5 の実施形態で検出できなかった画像の改ざん位置をより検出しやすくする効果がある。

#### 【 0 2 5 2 】

例えば、簡単な一例として、第 1 の特徴抽出部は離散ウェーブレット変換の低周波成分（L L）に基づく 2 次元特徴画像を抽出するとし、第 2 の特徴抽出部は離散ウェーブレット変換の高周波成分（H H）に基づく 2 次元特徴画像を抽出するとよい。2 次元特徴画像は、画像領域 B の情報量に応じて、画像領域 B に収まるように階調数を減らす必要があるが、低周波成分と高周波成分の両方を 2 次元特徴画像に含ませることで、双方において改ざん前後で変化しない改ざん画像を生成することを難しくし、画像の改ざん位置を検出し易くすることが出来る。

#### 【 0 2 5 3 】

また、第 1 の特徴抽出部は多値の縮小画像を 2 次元特徴画像として抽出するとし、第 2 の特徴抽出部は画像の輪郭を 2 次元特徴画像として抽出するとする。この場合にも、画像全体で平均値を維持しつつ、輪郭を変化がすることのない改ざん画像を生成することは難しく、画像の改ざん位置をより検出し易くすることが

出来る。

#### 【 0 2 5 4 】

その場合、透かし情報には夫々の 2 次元特徴画像が含まれていると共に、夫々の 2 次元特徴画像がどのような処理により生成されたものであるかを示す情報が含まれている。

#### 【 0 2 5 5 】

そして改竄位置検出装置は、改竄画像に対して同様に複数の 2 次元特徴画像を生成し、透かし情報から抽出した夫々の 2 次元特徴画像と、改竄画像から生成された夫々の 2 次元特徴画像とで夫々対応する画像同士（同じ抽出処理により得られた画像同士）を比較することで、改竄の位置を検出することができる。

#### 【 0 2 5 6 】

なお、本実施形態に係る処理は、上記各実施形態に適用しても良い。

#### 【 0 2 5 7 】

##### [第 7 の実施形態]

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データが J P E G 圧縮符号化データである場合について考える。J P E G 圧縮符号化方式は、既によく知られている符号化方式の為、詳しい説明はここでは省略する。

#### 【 0 2 5 8 】

図 1 2 は画像の一部（ $8 \times 8$  画素）の領域に対して、離散コサイン変換を実行し、所定の量子化テーブルで量子化した D C T 量子化係数を 2 次元的に表している図である。

#### 【 0 2 5 9 】

同図に示した各係数配置において、左上には直流成分（D C， $8 \times 8$  画素の平均値）が配置されており、その他の位置には夫々固有の周波数成分が配置されている。

#### 【 0 2 6 0 】

J P E G 圧縮符号化データに対して、第 1 ～ 第 4 の実施形態で述べた改ざん位置検出用電子透かしを埋め込む場合、各  $8 \times 8$  ブロックにおいて、画質への影響が少ない周波数成分を電子透かしの埋め込み対象である画像領域 B としてランダ

ムに1つもしくは複数選択し、残りの領域を画像領域Aするとよい。例えば、図12のように1202は画像領域B、その他の周波数成分は画像領域Aとすることが出来る。

#### 【0261】

2次元特徴画像を生成する際には画像領域Aの中で直流成分（DC成分）のみを処理の対象として2値画像を生成し、ダイジェストを生成する際には画像領域Aにある全てのデータを利用するとよい。この場合、JPEG圧縮符号化画像で輝度や色の変更が起きた場合でも、改ざん位置の特定を行うことが可能である。

#### 【0262】

##### [第8の実施形態]

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データがJPEG2000圧縮符号化画像データである場合について考える。

#### 【0263】

JPEG2000圧縮符号化方式は既によく知られている符号化方式の為、詳しい説明はここでは省略する。JPEG2000圧縮符号化方式では、入力画像夫々所定のサイズを有するタイルに分割し、タイル単位で離散ウェーブレット変換（DWT）を行い、複数の周波数帯域のサブバンドに分割する。図13は注目タイルに対して離散ウェーブレット変換を行うことで得られるDWT係数の配置を示す図である。左上のLLは画像に最も影響の大きい低周波成分を表すサブバンド、右下のHHは画像に影響が少ない高周波成分を表すサブバンドである。

#### 【0264】

JPEG2000圧縮符号化画像データに第1～第6の実施形態で述べた改ざん位置検出用電子透かしの埋め込みを行う一例を述べると、画像領域BとしてLLの最下位ビットプレーンを選択し、画像領域AとしてLLの最下位ビットプレーンを除くビットプレーンとして選択するとよい。この場合、LLを複数のビットプレーンからなる2次元画像とみなすことが出来るから、第1や第2の実施形態とはほぼ同様に改ざん位置検出用電子透かしの埋め込みと改ざん位置検出が実現できる。LLを操作する場合、画質劣化を生み易いが、高周波のサブバンドを取り除く圧縮に対しても改ざん位置を特定できる機能を維持することが出来る。



## 【0265】

また、その他の埋め込み方法として、画像領域BとしてLLを除く他の全てのサブバンド(HL1、HH1、LH1、HL2、HH2、LH2)とし、LLそのもの又はLLから得られる2次元特徴画像を画像領域Bに埋め込んでもよい。画像領域Bとしては、LLを除く他の全てのサブバンドではなく、(HL1、HH1、LH1、HL2、HH2、LH2)の中から所定のビットプレーンを選択する形としてもよい。画像領域Bに収める情報量が減るが、画像に対する劣化が抑えられるメリットがある。

## 【0266】

また、離散ウェーブレット変換を実行する最小単位であるタイル単位毎に画像領域Aおよび画像領域Bを選択して、改ざん位置検出用電子透かしの埋め込みと改ざん位置検出を行ってもよいが、タイル単位ごとではなく画像全体の複数のタイルにまたがる形で、画像領域Aおよび画像領域Bを選択し、改ざん位置検出用電子透かしの埋め込みと改ざん位置検出を行ってもよい。

## 【0267】

例えば、複数のタイルからLLのみを抽出し、最下位のビットプレーンを除く領域を画像領域A、最下位のビットプレーンを画像領域Bと設定する。この場合、既に第1乃至3の実施形態で述べたように、画像領域Aから2次元特徴画像を生成し、透かし情報を生成し、透かし情報に対し暗号化処理、誤り訂正符号化処理、インターリーブ処理を行うことで得られる透かし情報を画像領域Bと置き換えればよい。

## 【0268】

## [第9の実施形態]

本実施形態では、改ざん位置検出用電子透かしの埋め込みを行う画像データがMPEGやMotion JPEG、Motion JPEG2000に代表される動画データである場合について考える。MPEGは基本的にはJPEG圧縮符号化で用いた離散コサイン変換に基づく圧縮をベースとしており、第7の実施形態で述べたJPEG圧縮符号化画像の改ざん位置検出用電子透かしの埋め込み方法を、時間軸に拡張し、画質への影響が少ないDCT係数を適当に選択すること

により、適用可能である。

#### 【0269】

Motion JPEGやMotion JPEG2000は、基本的にはJPEGやJPEG2000圧縮符号化画像を時間軸に重ねた構成となっており、第5、第6の実施形態で述べた手法を時間軸に拡張すれば、簡単に適用することが可能である。

#### 【0270】

また上記実施形態に係る処理の対象として音声データを用いても良く、その場合、2次元特徴画像を1次元特徴データに置き換えることで適応可能である。

#### 【0271】

##### [第10の実施形態]

本実施形態では、上記第1乃至9の実施形態に係る夫々の処理をコンピュータにより行わせる。図14は、上記第1乃至9の実施形態に係る埋め込み装置、改竄位置検出装置として機能するコンピュータの基本構成を示す図である。例えばこのコンピュータを第1乃至3の実施形態に係る埋め込み装置、改竄位置検出装置として機能させる場合、図1、4、9、10、17に示した各機能構成をプログラムにより表現し、このコンピュータに読み込ませることで、このコンピュータを第1乃至3の実施形態に係る埋め込み装置、改竄位置検出装置として機能させることができる。

#### 【0272】

また、埋め込み装置、改竄位置検出装置は夫々同一の装置としても良いし、別個の装置としても良い。

#### 【0273】

同図において、1411はCPUで、RAM1412やROM1413に格納されているプログラムやデータを用いて、コンピュータ全体の制御を行うと共に、上記各実施形態で説明した各処理を行う。

#### 【0274】

1412はRAMで、外部記憶装置1418からロードされたプログラムやデータ、他のコンピュータシステム1424からI/F（インターフェース）14

23を介してダウンロードしたプログラムやデータを一時的に記憶するエリアを備えると共に、CPU1411が各種の処理を行うために必要とするエリアを備える。

#### 【0275】

1413はROMで、コンピュータの機能プログラムや設定データなどを記憶する。1414はディスプレイ制御装置で、画像や文字等をディスプレイ1415に表示させるための制御処理を行う。1415はディスプレイで、画像や文字などを表示する。なお、ディスプレイとしてはCRTや液晶画面などが適用可能である。

#### 【0276】

1416は操作入力デバイスで、キーボードやマウスなど、CPU1411に各種の指示を入力することのできるデバイスにより構成されている。なお手動で上記秘密鍵や公開鍵などを入力する場合には、この操作入力デバイス1416を介してこれらを入力することができる。1417は操作入力デバイス1416を介して入力された各種の指示等をCPU1411に通知するためのI/Oである。

#### 【0277】

1418はハードディスクなどの大容量情報記憶装置として機能する外部記憶装置で、OS（オペレーティングシステム）や上記各実施形態に係る処理をCPU1411に実行させるためのプログラム、埋め込み情報を埋め込む対象となる画像データなどを記憶する。また、秘密鍵を予め保存しておいても良い。外部記憶装置1418への情報の書き込みや外部記憶装置1418からの情報の読み出しはI/O1419を介して行われる。

#### 【0278】

1421は画像を撮像するためのデジタルカメラで、撮像した画像はI/O1422を介してRAM1412に出力、もしくは外部記憶装置1418に保存される。なお、画像を撮像するための機器はデジタルカメラに限定されるものではなく、例えば動画像を撮像するデジタルビデオカメラであってもよい。

#### 【0279】

1430はCPU1411、ROM1413、RAM1412、I/O1422、I/O1419、ディスプレイ制御装置1414、I/F1423、I/O1417を繋ぐバスである。

#### 【0280】

また、改ざん位置検出用電子透かし埋め込み・および改ざん位置検出を行う対象が音声信号の場合、デジタルカメラ1421の代わりにマイク等の音声入力機器をI/O1422に接続する。

#### 【0281】

なお本実施形態では、改ざん位置検出用電子透かしの埋め込み処理、改竄位置検出処理はコンピュータにより行っているが、改ざん位置検出用電子透かし埋め込み処理を、デジタルカメラ1421によって、専用のハードウェア回路を用いてデジタルデータの撮影直後に行わせ、CPU1411が改竄位置検出処理を行っても良い。もちろん、デジタルカメラ1421が改ざん位置検出用電子透かしの埋め込み処理を行ってもよい。

#### 【0282】

または、図示しないが音声に改ざん位置検出用電子透かしの埋め込む場合、音声入力機器に改ざん位置検出用電子透かしの埋め込み処理を行わせても良い。

#### 【0283】

上記各実施形態によれば、画像や動画、音声データに秘密の情報を用いることなく画像や動画、音声データの改ざん位置および改ざんの有無を検出することを可能にする。

#### 【0284】

なお、上記各実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

#### 【0285】

[その他の実施形態]

尚、本実施形態は、複数の機器（例えば、ホストコンピュータ、インターフェー

ス機器、リーダ、プリンタ等) から構成されるシステムに適用しても、一つの機器からなる装置 (例えば、複写機、ファクシミリ装置等) に適用してもよい。

#### 【0286】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体 (または記憶媒体) を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ (またはCPUやMPU) が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本実施形態を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム (OS) などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

#### 【0287】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

#### 【0288】

本実施形態を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートや機能構成に対応するプログラムコードが格納されることになる。

#### 【0289】

以下に、本発明の実施態様の例を示す。

#### 【0290】

〔実施態様 1〕 第 1 の領域と第 2 の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理装置であって、

前記第 1 の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成手段と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成手段と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化手段と、

前記原画像において、前記第 2 の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力手段と

を備えることを特徴とする画像処理装置。

#### 【 0 2 9 1 】

〔実施態様 2〕 更に、前記透かし情報生成手段が生成した透かし情報を暗号化する暗号化手段を備え、

前記誤り訂正符号化手段は、前記暗号化手段によって暗号化された透かし情報に対して誤り訂正符号化を行うことを特徴とする実施態様 1 に記載の画像処理装置。

#### 【 0 2 9 2 】

〔実施態様 3〕 前記暗号化手段は、前記透かし情報を公開鍵暗号化方式に従って暗号化することを特徴とする実施態様 2 に記載の画像処理装置。

#### 【 0 2 9 3 】

〔実施態様 4〕 更に、前記誤り訂正符号化透かし情報を構成するビット列を並び替える並び替え手段を備え、

前記誤り訂正符号化透かし情報は前記並び替え手段によってビット列が並び替えられたものであることを特徴とする実施態様 2 に記載の画像処理装置。

#### 【 0 2 9 4 】

〔実施態様 5〕 更に、前記第 1 の領域の画像を用いて、ハッシュ値を計算するハッシュ値計算手段を備え、

前記透かし情報生成手段は、前記透かし情報に更に前記ハッシュ値のデータを

含めることを特徴とする実施態様 1 乃至 4 の何れか 1 項に記載の画像処理装置。

【0 2 9 5】

〔実施態様 6〕 前記原画像に関する情報には、前記透かし情報が正しく復号されたか否かをチェックするために使用されるビット列が含まれることを特徴とする実施態様 1 に記載の画像処理装置。

【0 2 9 6】

〔実施態様 7〕 前記ビット列は少なくとも前記特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様 6 に記載の画像処理装置。

【0 2 9 7】

〔実施態様 8〕 前記原画像に関する情報には、前記特徴画像を生成する処理を特定する情報が含まれることを特徴とする実施態様 1 に記載の画像処理装置。

【0 2 9 8】

〔実施態様 9〕 前記特徴画像生成手段は、夫々異なる特徴抽出処理を行って前記原画像の特徴画像を複数生成することを特徴とする実施態様 1 に記載の画像処理装置。

【0 2 9 9】

〔実施態様 1 0〕 前記特徴画像は、前記原画像の部分画像であることを特徴とする実施態様 1 に記載の画像処理装置。

【0 3 0 0】

〔実施態様 1 1〕 第 1 の領域と第 2 の領域とで構成される改竄画像中の改竄の位置を検出する画像処理装置であって、

前記第 2 の領域に基づいた画像に対して誤り訂正復号を行い、前記改竄画像の改竄前の特徴を表す特徴画像と前記改竄画像の改竄前の画像に関する情報とを含む透かし情報を復元する誤り訂正復号手段と、

前記第 1 の領域の画像を用いて、前記改竄画像の特徴画像を生成する特徴画像生成手段と、

前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像と、前

記改竄画像の特徴画像とを用いて、前記改竄画像中の改竄の位置を通知する改竄位置通知手段と

を備えることを特徴とする画像処理装置。

#### 【0301】

〔実施態様 12〕 更に、前記第 2 の領域に基づいた画像を構成する、並び替えられたビット列を元の配置に復元する並び替え手段を備え、

前記誤り訂正復号手段は、前記並び替え手段によって並び替えられた前記第 2 の領域に基づいた画像に対して誤り訂正復号を行うことを特徴とする実施態様 11 に記載の画像処理装置。

#### 【0302】

〔実施態様 13〕 前記誤り訂正復号手段が復号した透かし情報が暗号化されている場合、当該暗号化されている透かし情報を復号し、当該透かし情報を復元する復元手段を備えることを特徴とする実施態様 11 又は 12 に記載の画像処理装置。

#### 【0303】

〔実施態様 14〕 前記復元手段は、前記暗号化された透かし情報を公開鍵暗号化方式に従って復号することを特徴とする実施態様 13 に記載の画像処理装置。

#### 【0304】

〔実施態様 15〕 前記改竄位置通知手段は、前記改竄画像の改竄前を表す画像と前記特徴画像との差分画像を生成し、当該差分画像を用いて前記改竄画像中の改竄の位置を通知することを特徴とする実施態様 11 又は 12 に記載の画像処理装置。

#### 【0305】

〔実施態様 16〕 更に、前記第 1 の領域の画像を用いて、ハッシュ値を計算するハッシュ値計算手段と、

前記ハッシュ値計算手段が計算したハッシュ値のデータと前記透かし情報に含まれるハッシュ値のデータとを比較し、前記改竄画像における改竄の有無を通知する改竄有無通知手段と



を備えることを特徴とする実施態様 11 に記載の画像処理装置。

**【0306】**

〔実施態様 17〕 前記改竄画像の改竄前の画像に関する情報には、前記暗号化されている透かし情報に対する改ざんの有無を判断するために、前記透かし情報の一部を検証する際に用いられるビット列が含まれることを特徴とする実施態様 13 に記載の画像処理装置。

**【0307】**

〔実施態様 18〕 前記ビット列は少なくとも前記改竄画像の改竄前の特徴を表す特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様 17 に記載の画像処理装置。

**【0308】**

〔実施態様 19〕 前記改竄画像に関する情報には、前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像を生成する処理を特定する情報が含まれることを特徴とする実施態様 11 に記載の画像処理装置。

**【0309】**

〔実施態様 20〕 前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像は、前記改竄画像の改竄前の部分画像であって、前記改竄画像の改竄前の画像に関する情報には、前記部分画像に関する情報が含まれることを特徴とする実施態様 11 に記載の画像処理装置。

**【0310】**

〔実施態様 21〕 前記特徴画像生成手段は、夫々異なる特徴抽出処理を行って前記第 1 の領域の画像の特徴画像を複数生成し、

前記改竄位置通知手段は、前記透かし情報に含まれる前記改竄画像の改竄前を表す夫々の画像と、前記特徴画像生成手段が生成した夫々の特徴画像とで、夫々対応する画像を用いて、前記改竄画像中の改竄の位置を通知することを特徴とする実施態様 12 に記載の画像処理装置。

**【0311】**

〔実施態様 22〕 前記改竄画像の改竄前の画像に関する情報には、当該情報を除く前記透かし情報全部の整合性を検証するためのビット列が含まれること

を特徴とする実施態様 1 3 に記載の画像処理装置。

#### 【0 3 1 2】

〔実施態様 2 3〕 前記ビット列は少なくとも前記改竄画像の改竄前の画像に関する情報を除く前記透かし情報全部に対するハッシュ値であることを特徴とする実施態様 2 2 に記載の画像処理装置。

#### 【0 3 1 3】

〔実施態様 2 4〕 更に、

前記ビット列を用いて、前記透かし情報に対する改ざんの有無を検出する検出手段と、

前記透かし情報に対する改ざんが検出されなかった場合に、前記誤り訂正復号手段によって誤り訂正される前の第 1 の暗号化されている透かし情報と、前記誤り訂正復号手段によって誤り訂正された後の第 2 の暗号化されている透かし情報とで対応するビット同士で、互いに異なるビット値であるビット同士の位置を示す比較画像を生成する比較手段と、

前記比較画像に基づき、前記改竄画像における改ざんの位置を通知する改竄位置通知手段と

を備えることを特徴とする実施態様 2 2 に記載の画像処理装置。

#### 【0 3 1 4】

〔実施態様 2 5〕 第 1 の領域と第 2 の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理装置であって、

予め作成された透かし情報を暗号化し、暗号化透かし情報を生成する暗号化手段と、

前記暗号化透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化暗号化透かし情報を生成する誤り訂正符号化手段と、

前記原画像において、前記第 2 の領域の画像情報を前記誤り訂正符号化暗号化透かし情報に置き換えた画像を出力画像として出力する出力手段と

を備えることを特徴とする画像処理装置。

#### 【0 3 1 5】

〔実施態様 2 6〕 前記暗号化手段は、前記透かし情報を公開鍵暗号化方式

に従って暗号化することを特徴とする実施態様 2 5 に記載の画像処理装置。

#### 【0 3 1 6】

〔実施態様 2 7〕 更に、前記誤り訂正符号化透かし情報を構成するビット列を並び替える並び替え手段を備え、

前記誤り訂正符号化透かし情報は前記並び替え手段によってビット列が並び替えられたものであることを特徴とする実施態様 2 5 に記載の画像処理装置。

#### 【0 3 1 7】

〔実施態様 2 8〕 前記透かし情報には、前記透かし情報が正しく復号されたか否かをチェックするために使用されるビット列が含まれることを特徴とする実施態様 2 5 に記載の画像処理装置。

#### 【0 3 1 8】

〔実施態様 2 9〕 前記ビット列は少なくとも前記特徴画像を含む透かし情報の一部に対するハッシュ値であることを特徴とする実施態様 2 8 に記載の画像処理装置。

#### 【0 3 1 9】

〔実施態様 3 0〕 第 1 の領域と第 2 の領域とで構成される改竄画像中の改竄の位置を検出する画像処理装置であって、

前記第 2 の領域に基づいた画像に対して誤り訂正復号を行い、誤りが訂正された第 2 の領域に基づいた画像を生成し、暗号化透かし情報を復元する誤り訂正復号手段と、

前記暗号化透かし情報を復号し、透かし情報を復元する暗号化復号手段と、

前記透かし情報の整合性を検証する透かし情報検証手段と、

前記透かし情報が整合性を満たしていれば、前記第 2 の領域に基づいた画像と誤りが訂正された第 2 の領域に基づいた画像を比較し、改ざん位置を検出する改ざん位置検出手段と

を備えることを特徴とする画像処理装置。

#### 【0 3 2 0】

〔実施態様 3 1〕 更に、前記第 2 の領域に基づいた画像を構成する、並び替えられたビット列を元の配置に復元する並び替え手段を備え、

前記誤り訂正復号手段は、前記並び替え手段によって並び替えられた前記第 2 の領域に基づいた画像に対して誤り訂正復号を行うことを特徴とする実施態様 3 0 に記載の画像処理装置。

### 【0 3 2 1】

[実施態様 3 2] 前記暗号化復号手段は、前記暗号化された透かし情報を公開鍵暗号化方式に従って復号することを特徴とする実施態様 3 0 に記載の画像処理装置。

### 【0 3 2 2】

[実施態様 3 3] 第 1 の領域と第 2 の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

前記第 1 の領域の画像を用いて、前記原画像の特徴画像を生成する特徴画像生成工程と、

前記特徴画像と前記原画像に関する情報とを含む透かし情報を生成する透かし情報生成工程と、

前記透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第 2 の領域の画像情報を前記誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

### 【0 3 2 3】

[実施態様 3 4] 第 1 の領域と第 2 の領域とで構成される改竄画像中の改竄の位置を検出する画像処理方法であって、

前記第 2 の領域に基づいた画像に対して誤り訂正復号を行い、前記改竄画像の改竄前の特徴を表す特徴画像と前記改竄画像の改竄前の画像に関する情報とを含む透かし情報を復元する誤り訂正復号工程と、

前記第 1 の領域の画像を用いて、前記改竄画像の特徴画像を生成する特徴画像生成工程と、

前記透かし情報に含まれる前記改竄画像の改竄前の特徴を表す特徴画像と、前記改竄画像の特徴画像とを用いて、前記改竄画像中の改竄の位置を通知する改竄

位置通知工程と

を備えることを特徴とする画像処理方法。

【0 3 2 4】

〔実施態様 3 5〕 第 1 の領域と第 2 の領域とで構成される原画像に対する改竄の位置を検出可能にするための情報を生成する画像処理方法であって、

予め作成された透かし情報を暗号化し、暗号化透かし情報を生成する暗号化工程と、

前記暗号化透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化暗号化透かし情報を生成する誤り訂正符号化工程と、

前記原画像において、前記第 2 の領域の画像情報を前記誤り訂正符号化暗号化透かし情報に置き換えた画像を出力画像として出力する出力工程と

を備えることを特徴とする画像処理方法。

【0 3 2 5】

〔実施態様 3 6〕 第 1 の領域と第 2 の領域とで構成される改竄画像中の改竄の位置を検出する画像処理方法であって、

前記第 2 の領域に基づいた画像に対して誤り訂正復号を行い、誤りが訂正された第 2 の領域に基づいた画像を生成し、暗号化透かし情報を復元する誤り訂正復号工程と、

前記暗号化透かし情報を復号し、透かし情報を復元する暗号化復号工程と、

前記透かし情報の整合性を検証する透かし情報検証工程と、

前記透かし情報が整合性を満たしていれば、前記第 2 の領域に基づいた画像と誤りが訂正された第 2 の領域に基づいた画像を比較し、改ざん位置を検出する改ざん位置検出工程と

を備えることを特徴とする画像処理方法。

【0 3 2 6】

〔実施態様 3 7〕 コンピュータを実施態様 1 乃至 3 2 の何れか 1 項に記載の画像処理装置として機能させることを特徴とするプログラム。

【0 3 2 7】

〔実施態様 3 8〕 コンピュータに実施態様 3 3 乃至 3 6 のいずれか 1 項に



記載の画像処理方法を実行させることを特徴とするプログラム。

【0328】

【実施態様39】 実施態様37又は38に記載のプログラムを格納することとを特徴とするコンピュータ読み取り可能な記憶媒体。

【0329】

【発明の効果】

以上の説明により、本発明によって、画像に対する改竄の位置を正確に検出することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図2】

1画素が8ビットから成る入力画像をビットプレーン毎に示した図である。

【図3】

入力画像、2次元特徴画像、そして後述するランダム化された誤り訂正符号化暗号化透かし情報によって表現される画像を示す図である。

【図4】

改ざん位置検出装置の機能構成を示すブロック図である。

【図5】

改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。

【図6】

透かし情報(601)、暗号化透かし情報(602)、誤り訂正符号化透かし情報(603)、ランダム化誤り訂正符号化透かし情報(604)のビット長を比較、説明するための概略図である。

【図7】

誤り訂正符号化を行う前の透かし情報C(w)の一例を示す図である。

【図8】

「透かし情報」の概略構成を示す図である。

【図 9】

本発明の第 2 の実施形態に係る改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図 1 0】

本発明の第 2 の実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。

【図 1 1】

本発明の第 2 の実施形態に係る改ざん位置検出処理の流れを示すフローチャートである。

【図 1 2】

画像の一部（ $8 \times 8$  画素）の領域に対して、離散コサイン変換を実行し、所定の量子化テーブルで量子化した D C T 量子化係数を 2 次元的に表している図である。

【図 1 3】

注目タイルに対して離散ウェーブレット変換を行うことで得られる D W T 係数の配置を示す図である。

【図 1 4】

本発明の第 1 乃至 8 の実施形態に係る埋め込み装置、改竄位置検出装置として機能するコンピュータの基本構成を示す図である。

【図 1 5】

論文（1）における改ざん位置検出用電子透かし埋め込み装置の機能構成を示すブロック図である。

【図 1 6】

論文（1）における改ざん位置検出装置の機能構成を示すブロック図である。

【図 1 7】

本発明の第 3 の実施形態に係る改ざん位置検出装置の機能構成を示すブロック図である。

【図 1 8】

第 2 改ざん位置検出部 1 7 0 0 の機能構成を示すブロック図である。

【図 1 9】

本発明の第 3 の実施形態に係る改ざん位置検出処理の流れを示すフローチャートである。

【図 2 0】

図 1 9 のステップ A 1 （ステップ S 1 9 1 0）の詳細を示すフローチャートである。

【図 2 1】

図 1 9 のステップ A 2 （ステップ S 1 9 2 0）の詳細を示すフローチャートである。

【図 2 2】

改ざんが行われた改ざん画像から改ざん位置を判定する処理を説明するための図である。

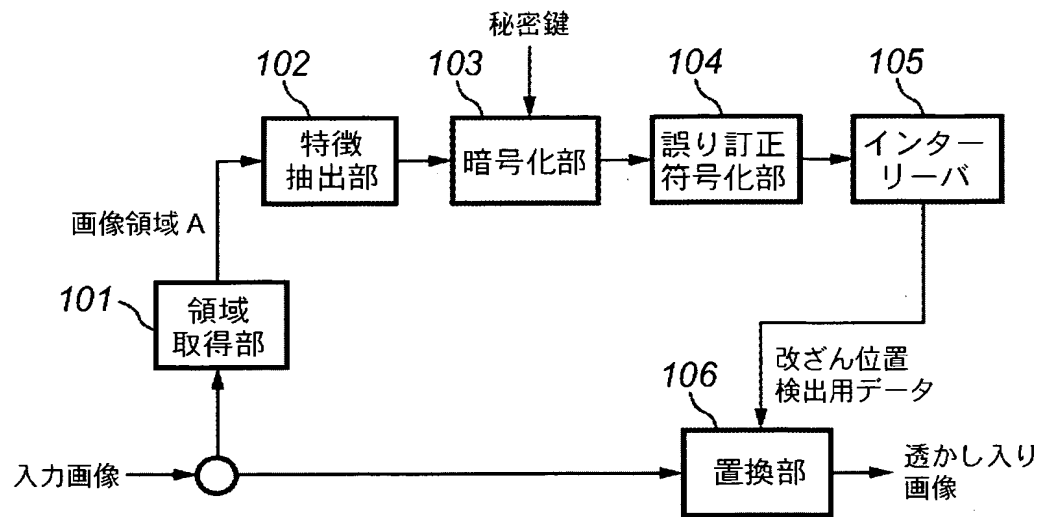
【図 2 3】

第 2 改ざん位置特定ビット系列 S （B S）と改ざん画像との対応を示す図である。

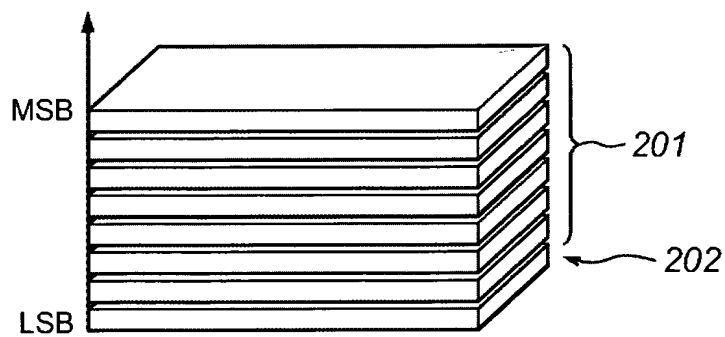


【書類名】 図面

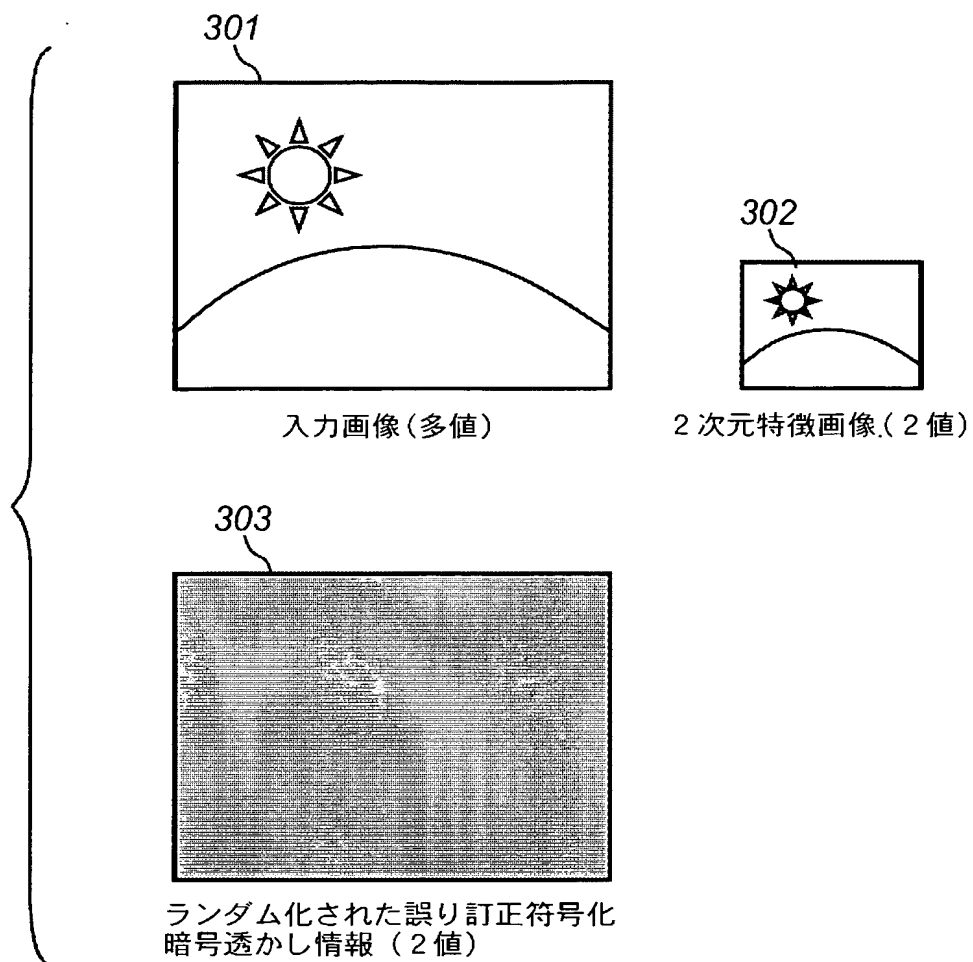
【図 1】



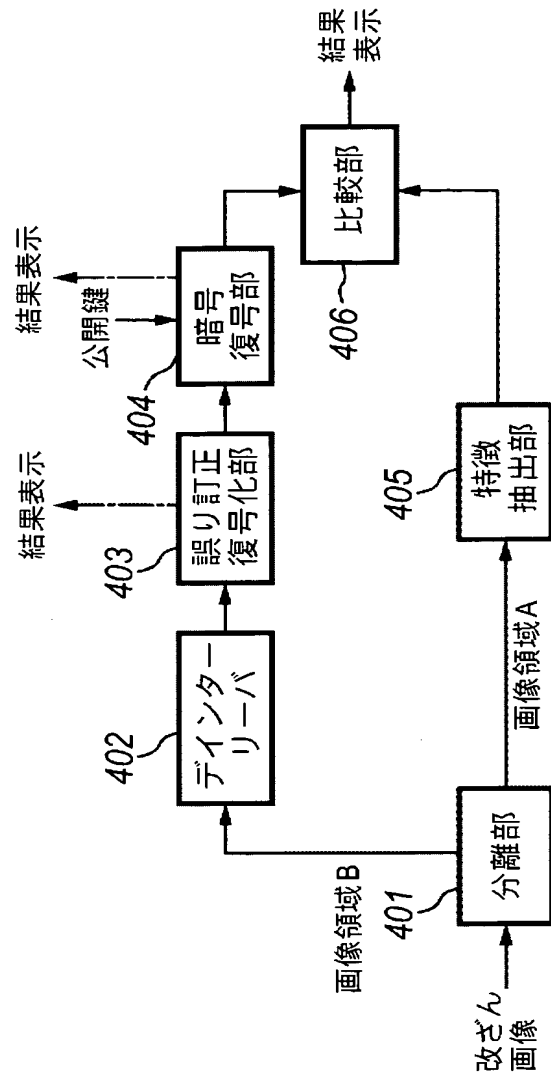
【図 2】



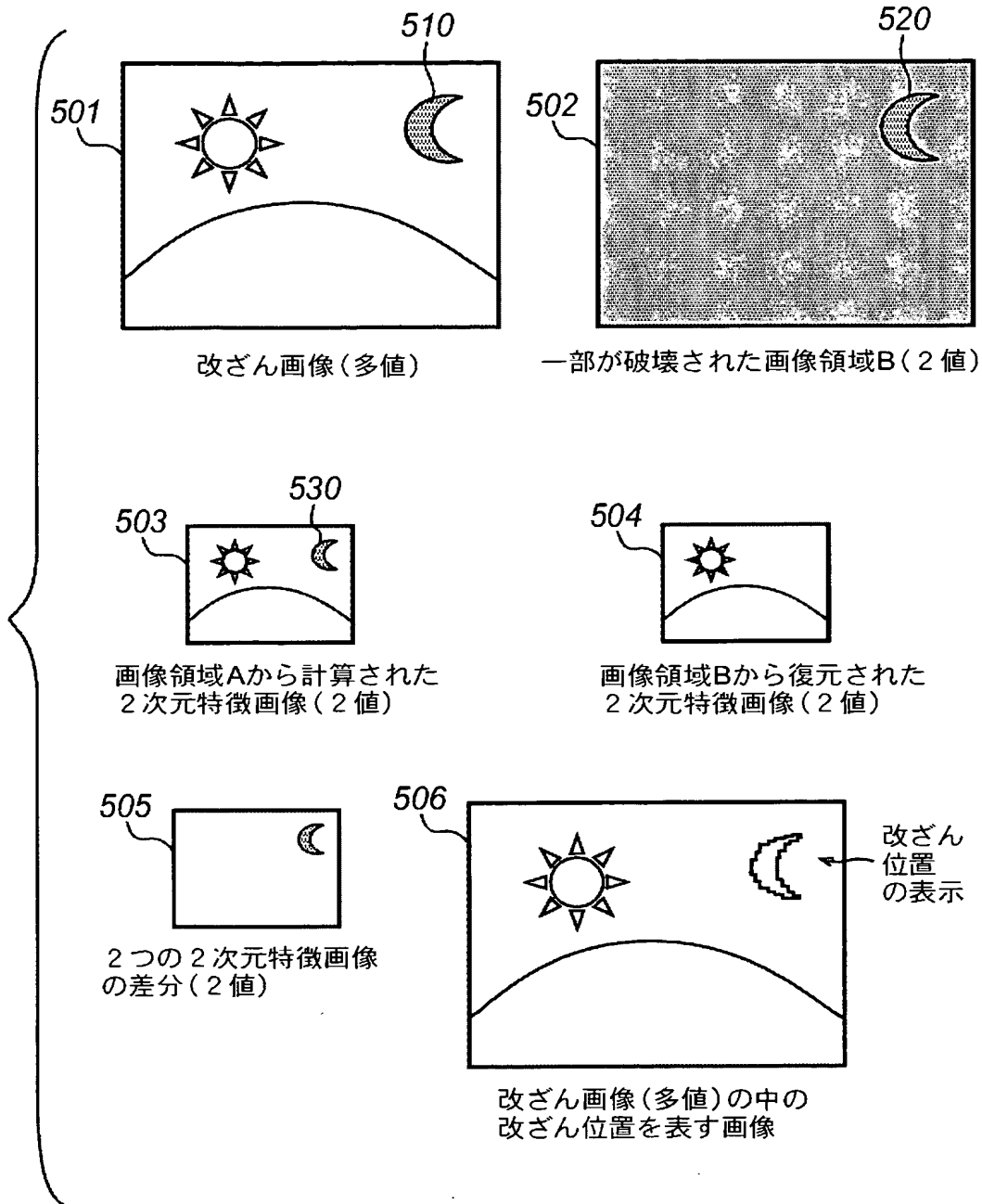
【図 3】



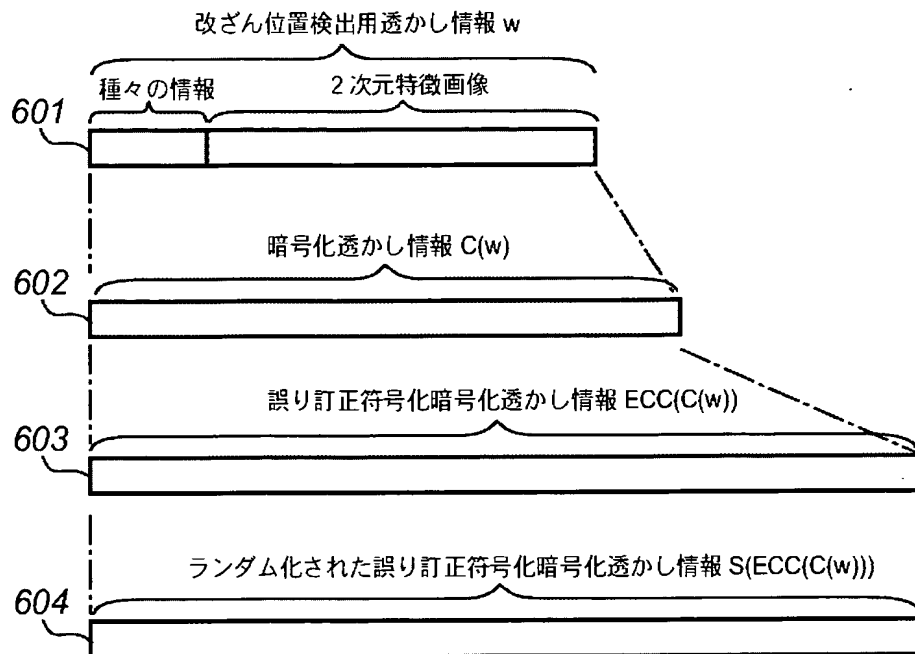
【図 4】



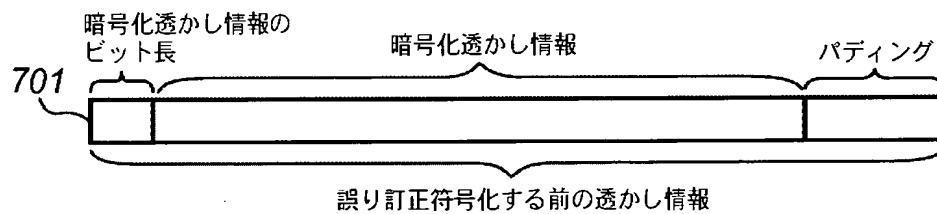
【図 5】



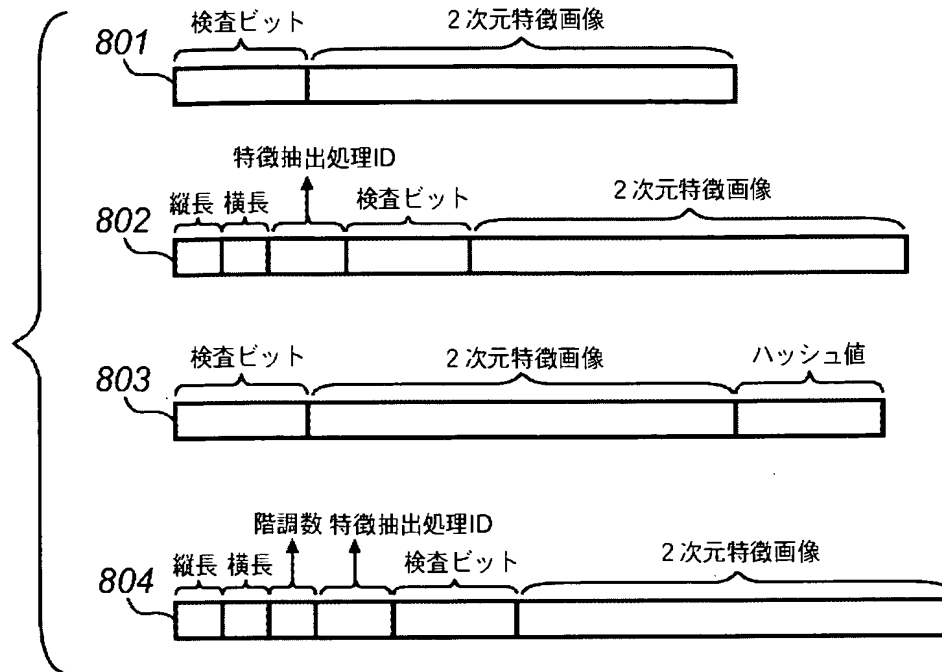
【図 6】



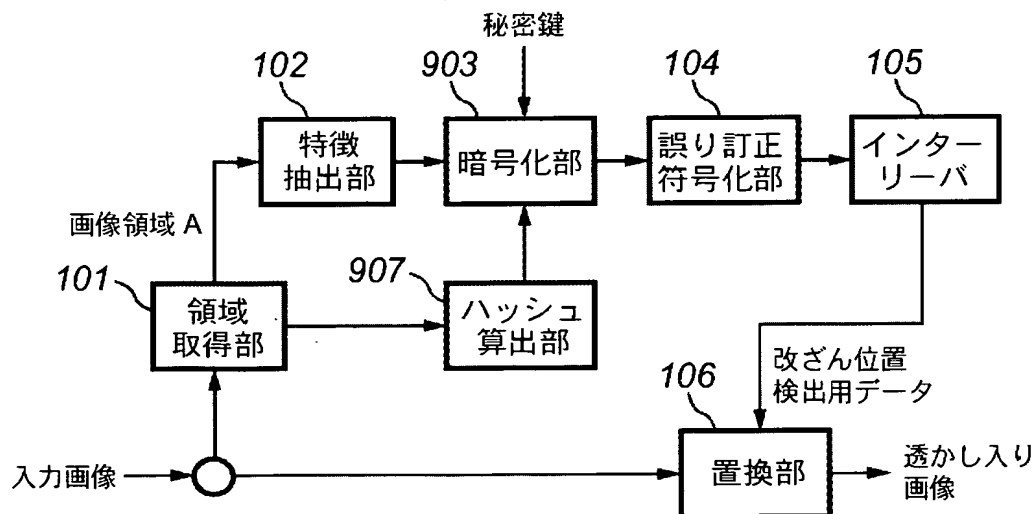
【図 7】



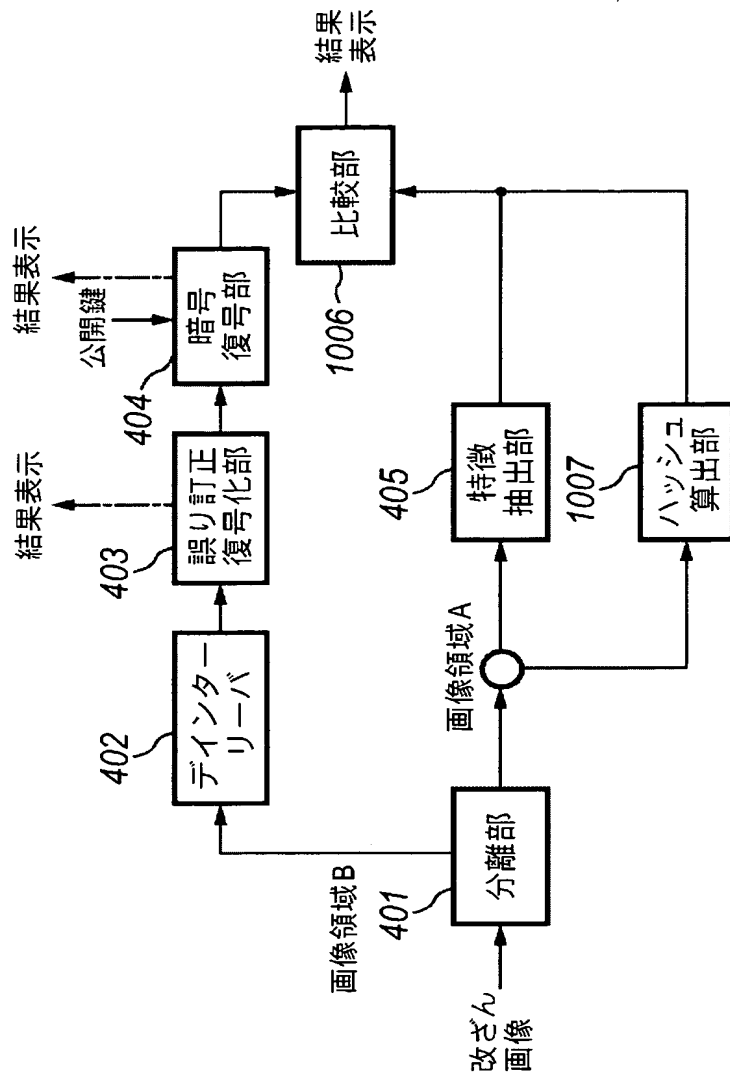
【図 8】



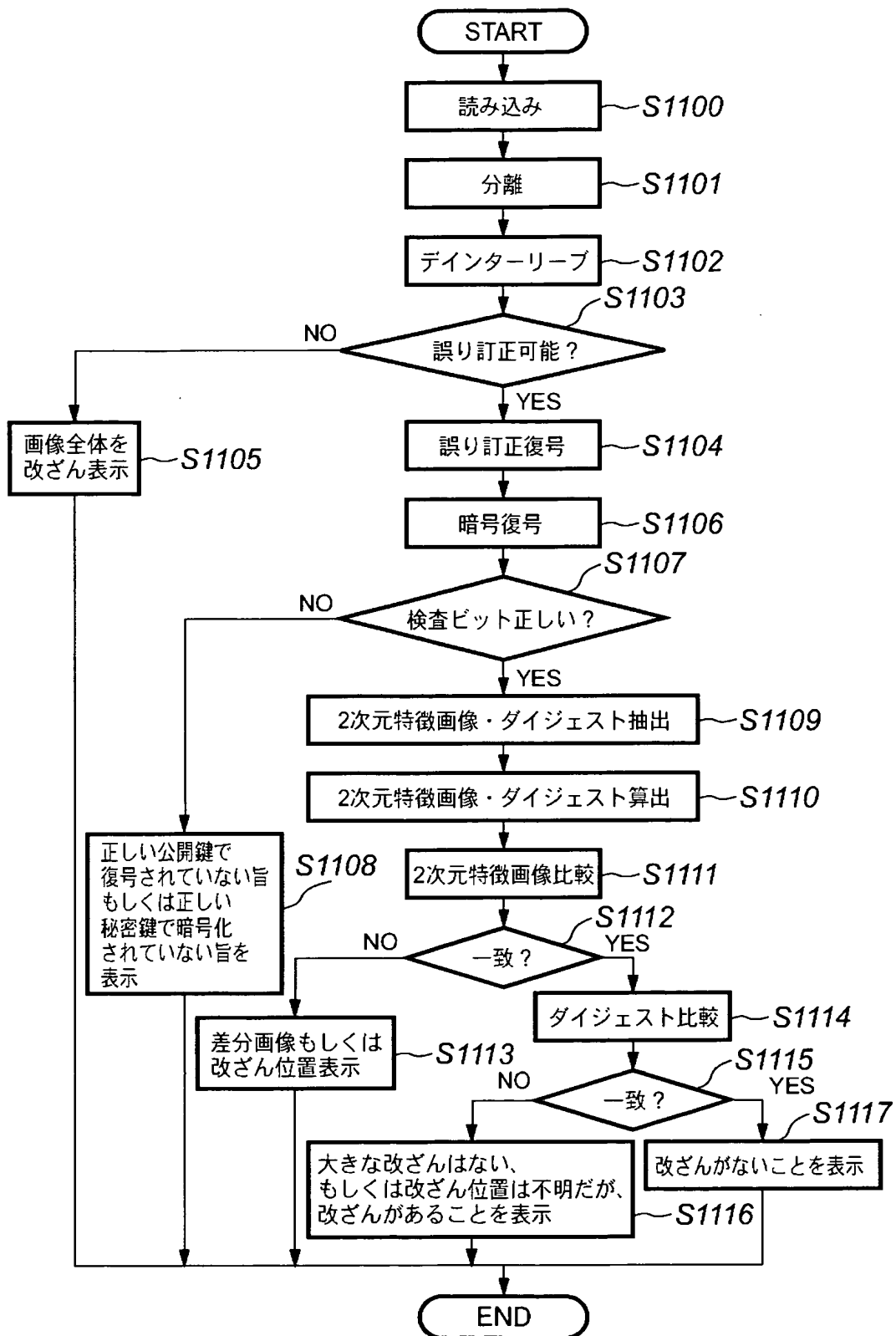
【図 9】



【図 10】

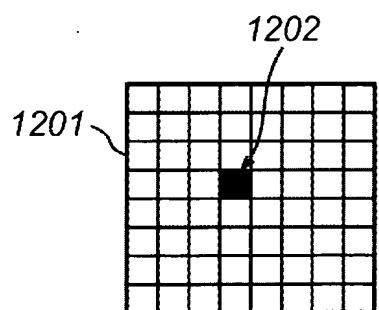


【図 11】



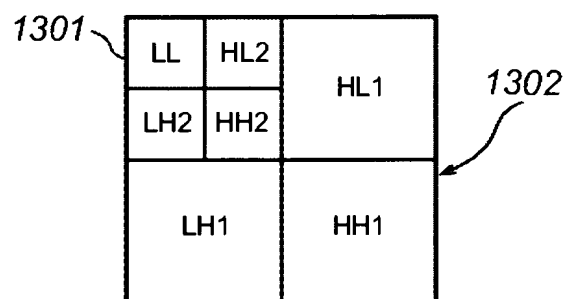


【図 1 2】

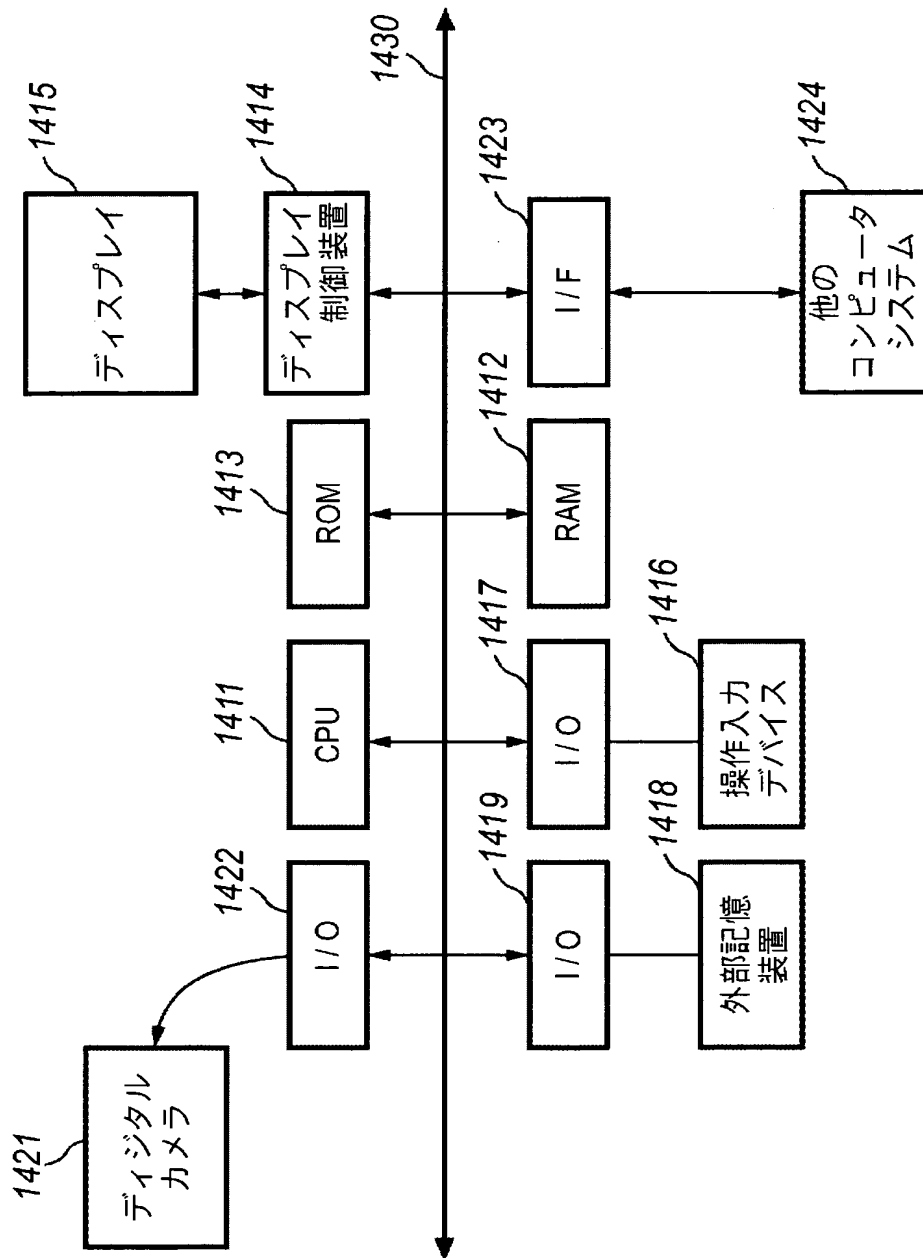


DCT量子化係数

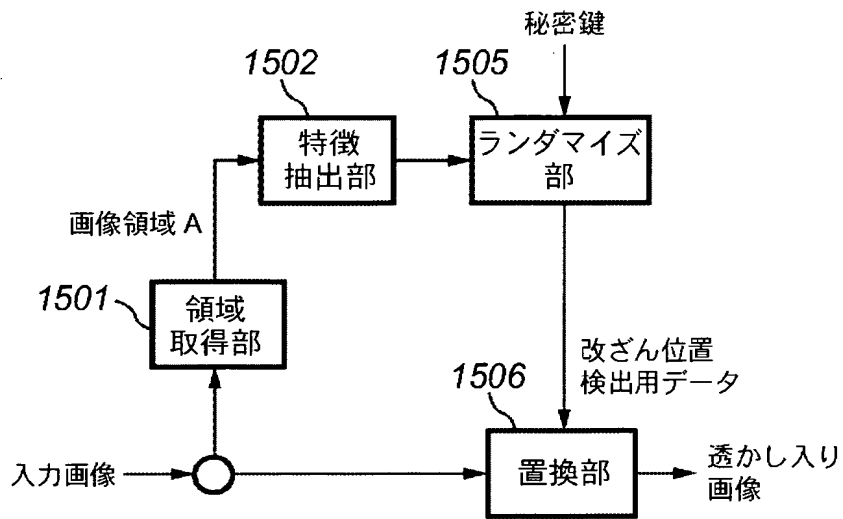
【図 1 3】



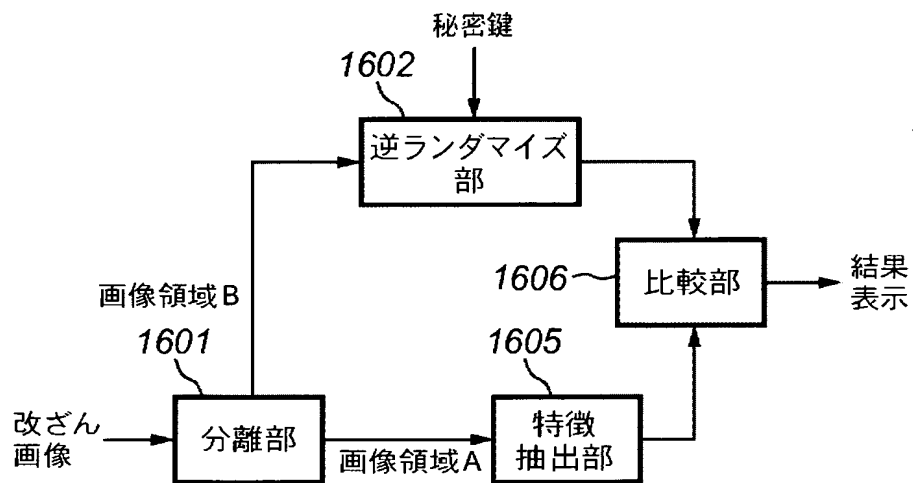
【図 14】



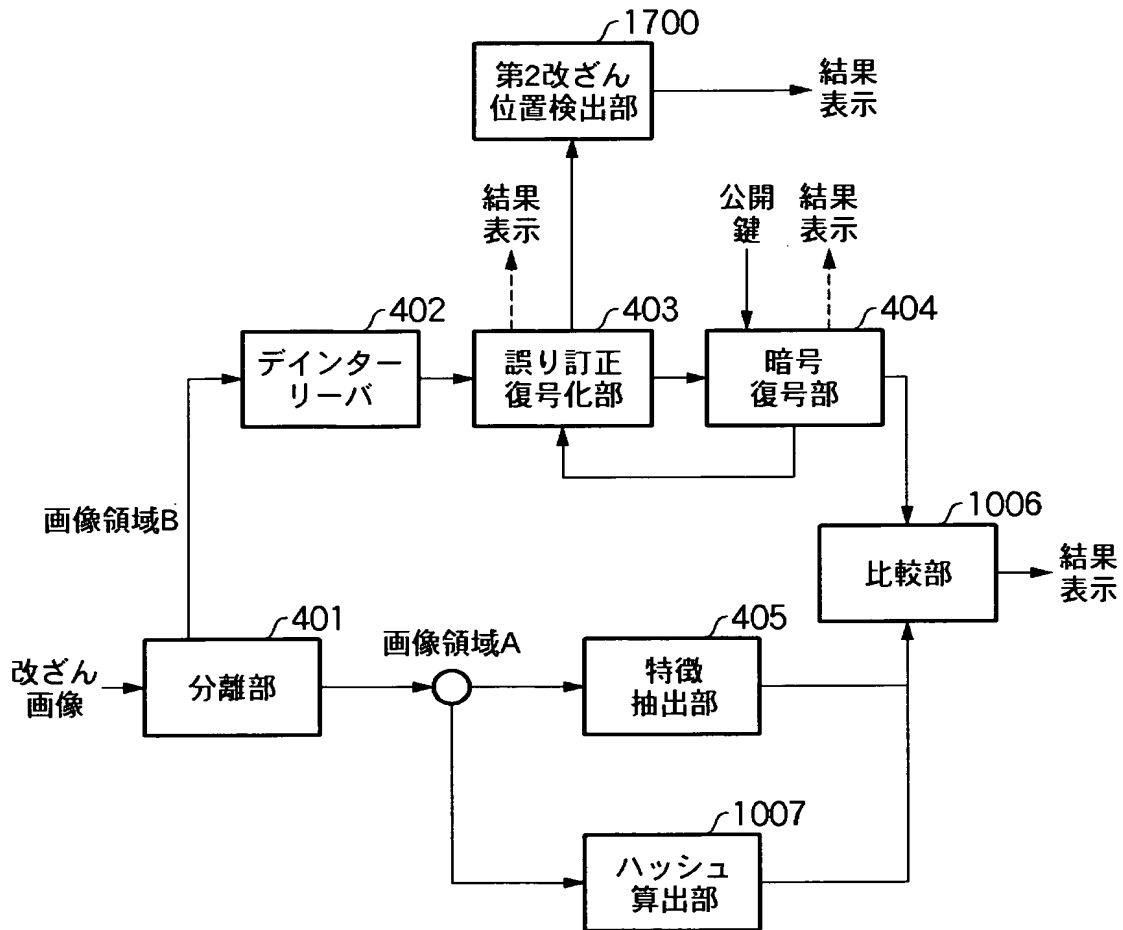
【図 15】



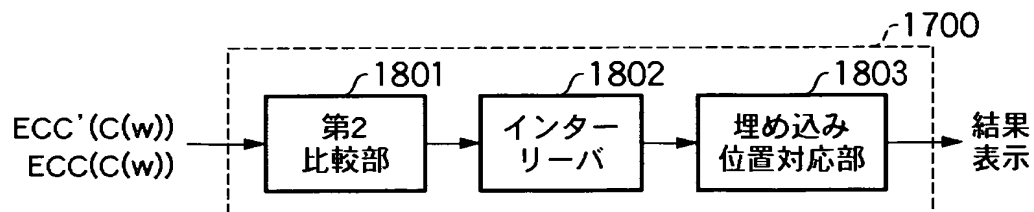
【図 16】



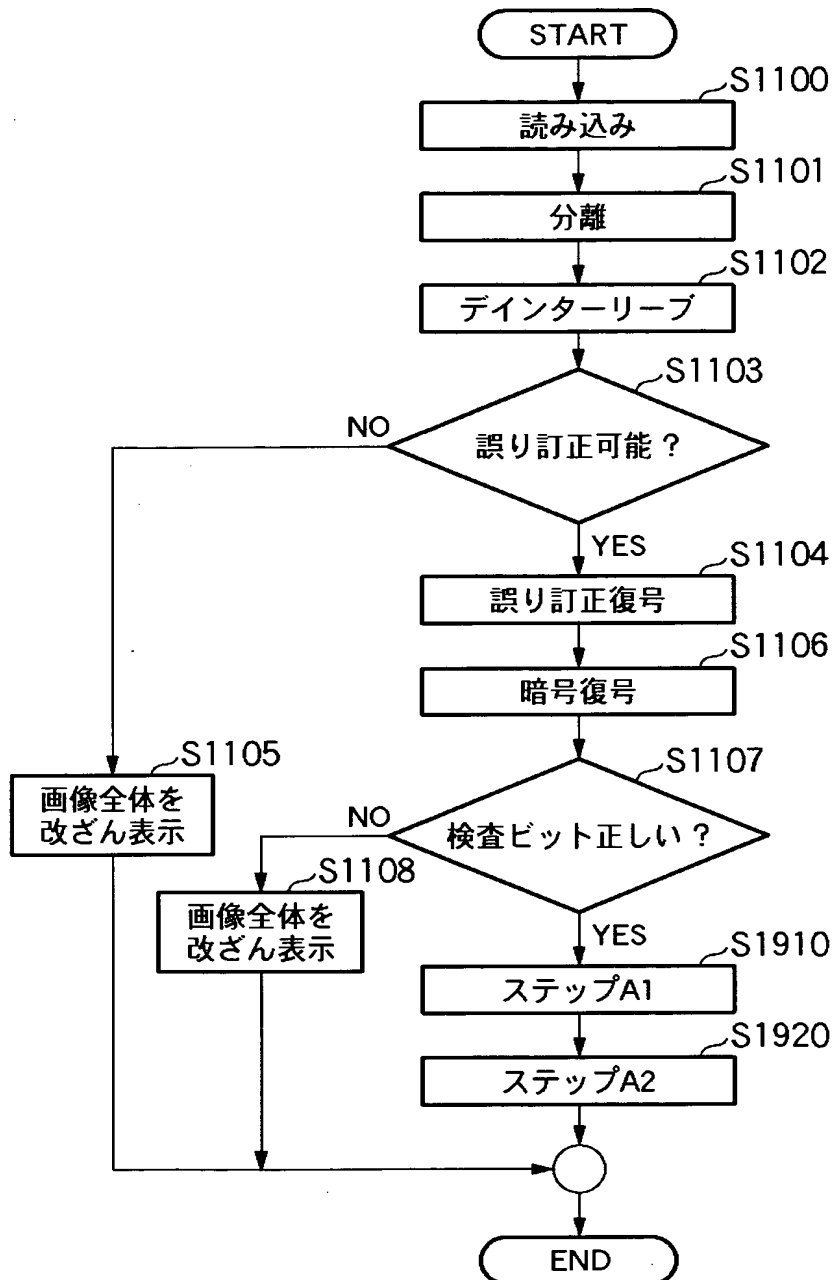
【図 17】



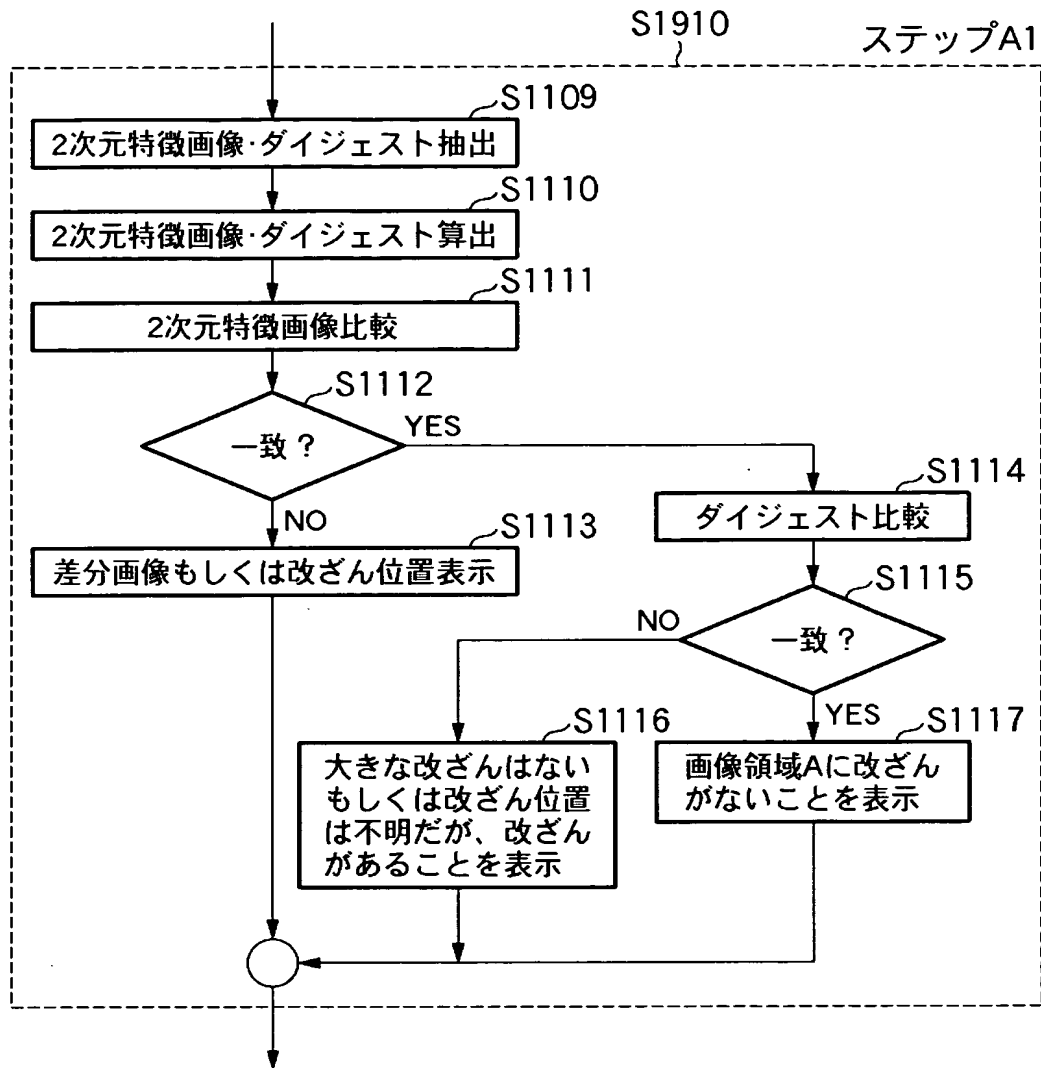
【図 18】



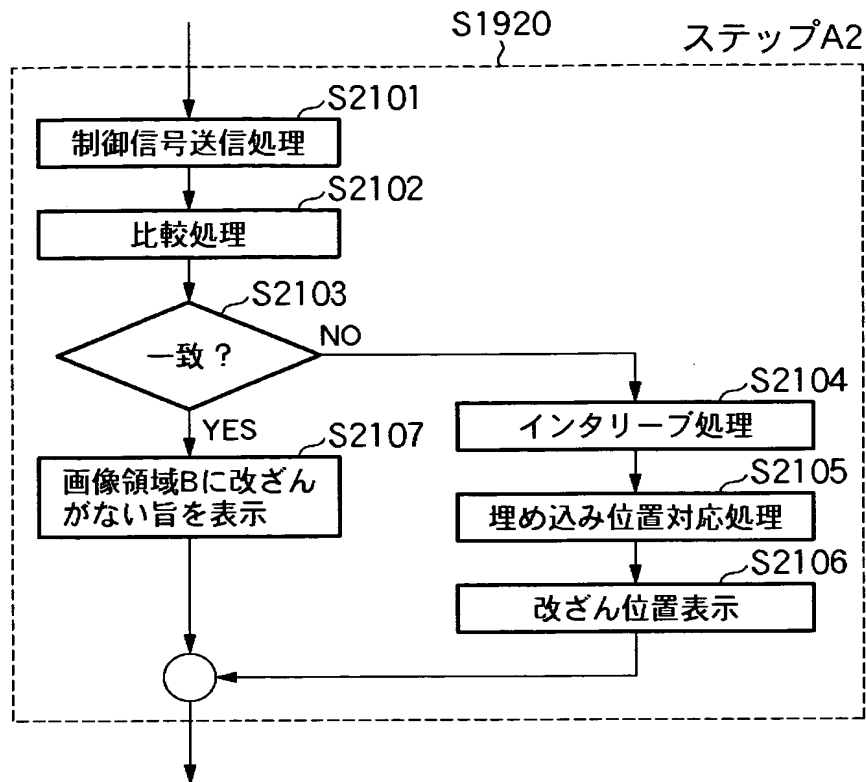
【図 19】



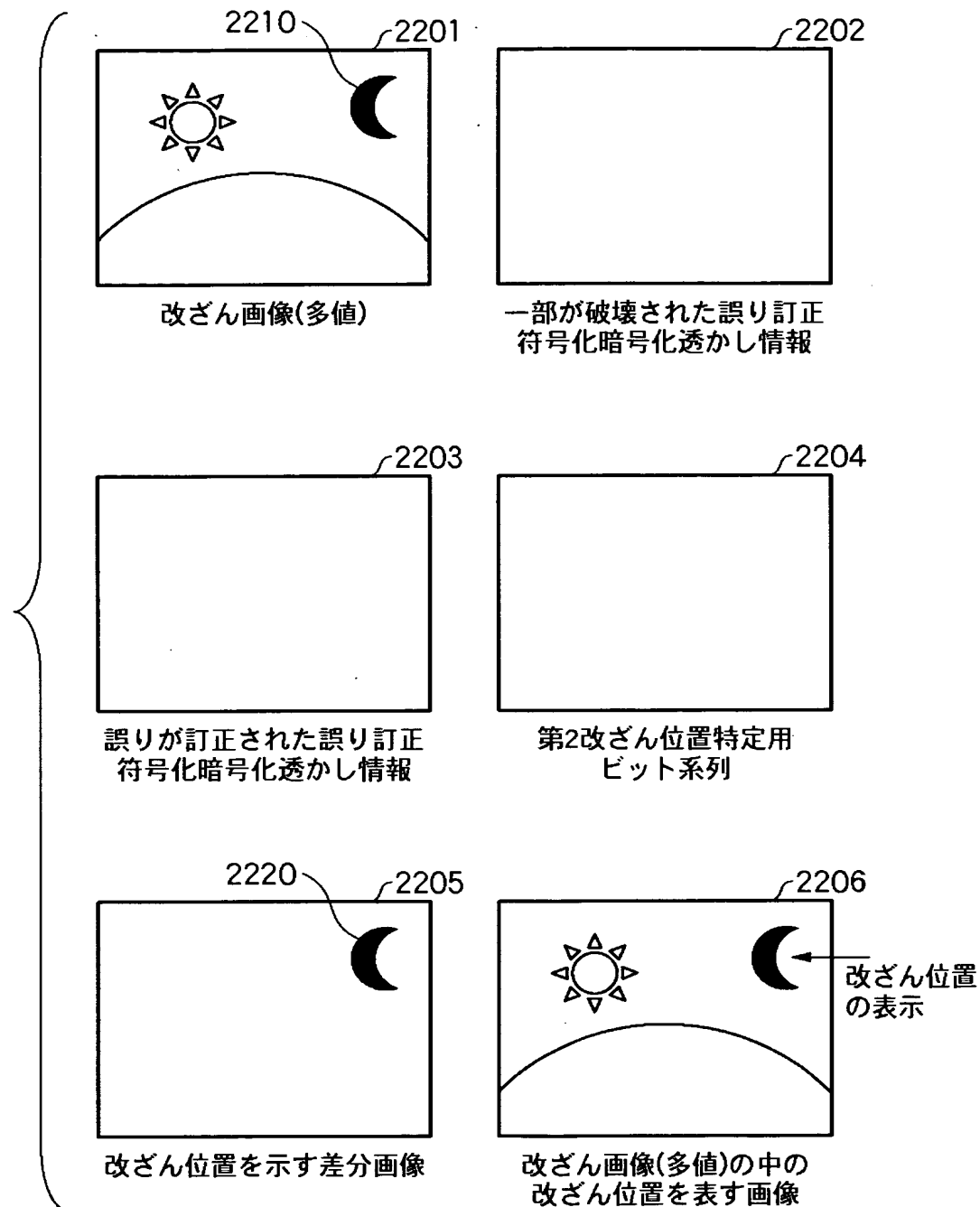
【図 20】



【図 2 1】

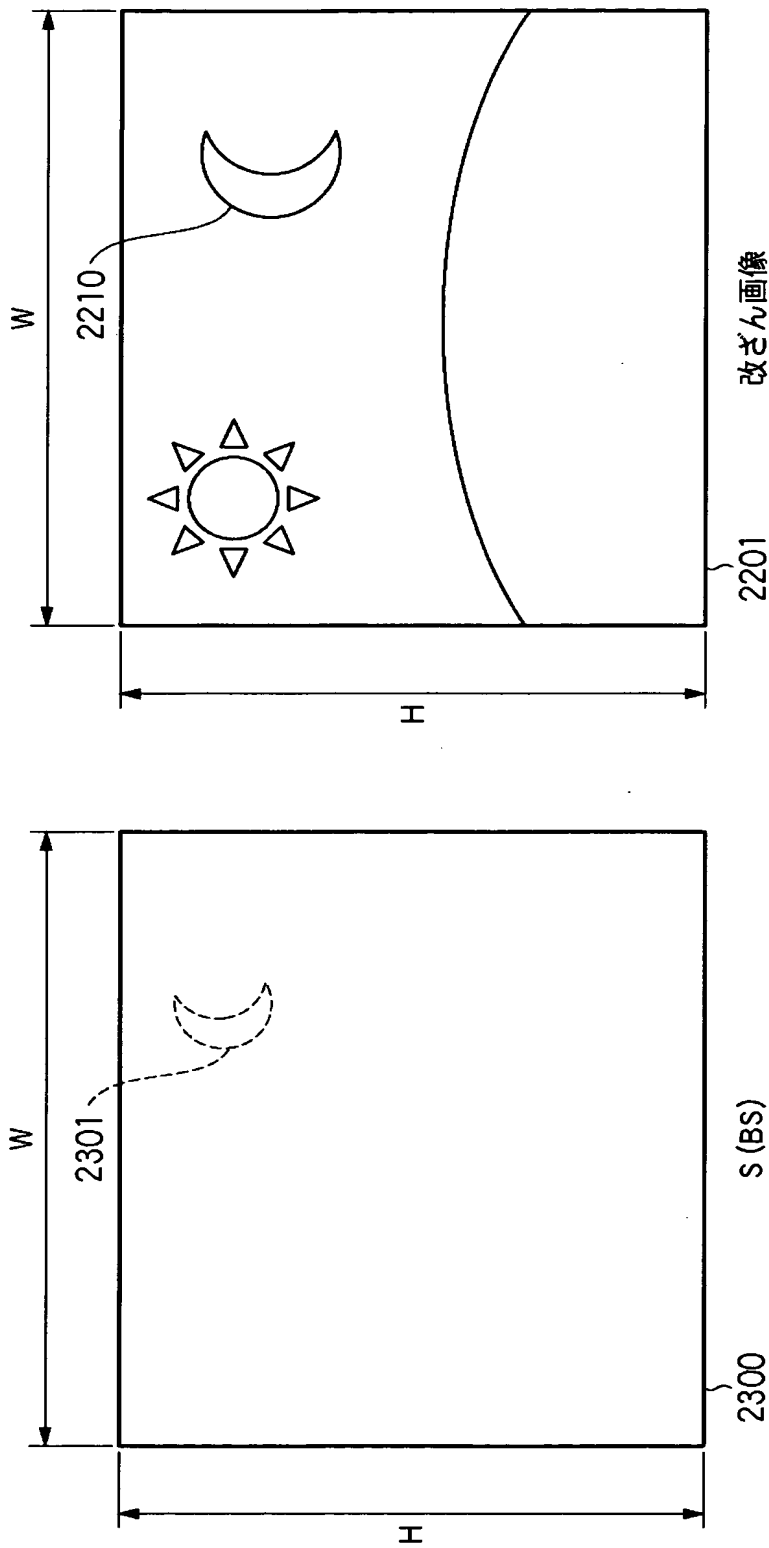


【図 22】





【図 2 3】



【書類名】 要約書

【要約】

【課題】 画像に対する改竄の位置を正確に検出すること。

【解決手段】 特徴抽出部 1 0 2 は、第 1 の領域と第 2 の領域とで構成される原画像中の第 1 の領域の画像を用いて、原画像の特徴画像を生成し、暗号化部 1 0 3 は特徴画像と原画像に関する情報とを含む透かし情報を生成する。そして誤り訂正符号化部 1 0 4 は、透かし情報に対して誤り訂正符号化を行い、誤り訂正符号化透かし情報を生成し、置換部 1 0 6 は原画像において、第 2 の領域の画像情報を誤り訂正符号化透かし情報に置き換えた画像を出力画像として出力する。

【選択図】 図 1

## 認定・付加情報

特許出願の番号	特願 2003-105498
受付番号	50300589240
書類名	特許願
担当官	第七担当上席 0096
作成日	平成 15 年 4 月 14 日

## &lt;認定情報・付加情報&gt;

## 【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子 3 丁目 30 番 2 号
【氏名又は名称】	キヤノン株式会社

## 【代理人】

申請人

【識別番号】	100076428
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	大塚 康徳

## 【選任した代理人】

【識別番号】	100112508
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	高柳 司郎

## 【選任した代理人】

【識別番号】	100115071
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	大塚 康弘

## 【選任した代理人】

【識別番号】	100116894
【住所又は居所】	東京都千代田区紀尾井町 3 番 6 号 秀和紀尾井町 パークビル 7 F 大塚国際特許事務所
【氏名又は名称】	木村 秀二

次頁無

特願 2 0 0 3 - 1 0 5 4 9 8

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 1 0 0 7 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社